CERT Orange Polska 2018 Report

secured by
CyberTarcza

orange™

The report was developed in cooperation with Integrated Solutions, the supplier of modern ICT solutions.

Table of Contents

It seems obvious that most of us are perfectly aware of what we shouldn't click and where we shouldn't enter our personal data. However, statistics show that there's still a lot to be done in that matter. That's why we have constantly been educating on the basics of safe internet through CERT Orange Polska activities, our blog posts, conference talks, and also Orange Foundation programs. We also develop services and tools, that help all of us to minimize the threats. As promised, we launched mobile CyberTarcza, following the one that has been protecting home internet users for the past 4 years (2.5 mln attempts were secured just in 2018).

What did the world of cyberthreats look like in 2018 from Orange Polska perspective? I hope you'll enjoy the 5th edition of CERT Orange Polska report.

Jean-François Fallacher
President of the Management Board
Orange Polska

5 billions of Internet of Things devices connected to the internet when we were publishing the first issue of our report. By 2020, the number is expected to grow to 20 billions.

1. Cybersecurity on 5

February 2014 - we won't forget that date at Orange Polska for a long time. An attack on tens of thousands of modems in the Polish network, temporarily disconnecting the infected devices from the internet to provide safety for their users… This cyberthreat, whose scale was the biggest ever in our country, was not only the root cause to create CyberTarcza, but – what is equally important – motivated us to share our cybersecurity experience with others in Poland and across the world. A year later we published the first CERT Orange Polska report.

5 years passed in an instant. And throughout this time the world has changed, the internet and its threats have changed, as well as your approach to cybersecurity. We have also matured. The first issue of our report was a "probe" to check how much the market is interested in this specific topic. Every year, we have not only tried to provide you with an analysis based on thorough data from Orange Polska network, but also to enrich each issue of the report with the experts' point of view on various aspects of cybersecurity.

Ransomware, Internet of Things: these issues were talked about rarely – if at all – 5 years ago. Now they are becoming crucial in the cybersecurity world. There are no worthless targets for cyber criminals. Each and all of us can become a victim, just because it's easier to rob a thousand people from 1000 PLN each than to steal 1 mln PLN from a company that is well prepared and equipped with cybersecurity tools.

There were 5 bilion of Internet of Things devices connected to the internet when we were publishing the first issue of our report. By 2020, the number is expected to grow to 20 bilion. It is a great challenge for us.

A cyber-criminal today is more of a psychologist than a malware specialist – that's why the chapter on "how not to get fooled" is the vital one in the report. Cybersecurity today is so much more than just an antivirus or firewall on our home computer. We can avoid the majority of threats if we just use common sense.

Commentary

Arnaud Martin
Orange Group CISO

CERT Orange Polska is one of the four major Security Operations Center of Orange Group. They play a central role in the security of Orange Polska, but as well we rely on their competencies for the protection of part of European and MEA Orange Divisions. In 2018, they faced massive DDoS attacks (more than hundreds Gbps on fix and mobile networks), they monitored hundreds of thousands events per second with their SIEM tools, they handled thousands of security incidents, they realized hundreds of audits to prevent potential vulnerabilities on services launched on Orange polish services. To be able to protect us against the exponential increasing security threats worldwide, the most important thing is not only the technical arsenal owned by the SOC but the individual expertise and the collective intelligence of the team.

Over the last 20 years, Orange Polska has invested continuously in security, building solutions from scratch such as the CyberTarcza success, using commercial leader's solutions and stimulating the innovation with startups such as SecBI and Morphisec. They invested as well in developing the security awareness at different level: internally in Orange Polska to be able to introduce security by design in each Line of Business, globally in Poland by playing a role in various user groups, promoting best practices on their website (https://cert.orange.pl/) and in the whole Orange group by becoming active members of the Security Expert Community and participating to the last internal Capture The Flag (CTF'18) challenge.

This mix within the team between technical expertise and human sensitivity is the key factor to succeed in security. With the introduction on May 25th 2018 of the EU General Data Protection Regulation (GDPR), security was reinforced as a pillar of our digital life and footprint. For Orange, the protection of every citizens' data is not only a legal commitment, but a company collective engagement where CERT Polska is playing a central role: with our CyberDefense team, we commit to protect your essentials.

Let's now have a look at what happened in 2018 in details and how we are preparing 2019!

2. Security incidents handled by CERT Orange Polska

We present the percentage distribution of incidents we handled manually in 2018. The incidents concerned online service networks. We have divided our analysis into nine categories, and compared it with the previous year.

The incidents processed included attacks on resources connected with the Orange Polska network, as well as the ones conducted using the network's own resources. They affected all kinds of networks in terms of their end user, meaning both individual users, and corporate subjects. Information about the incidents was coming both from external sources and internal security systems. External sources mostly include user reports, but also information coming from security organizations and other CSIRT-type units. Our security systems consist of i.a. intrusion detection/prevention systems (IDS/IPS), network traffic analysers looking for DDoS attacks and malicious code, honeypots, security information and event management systems (SIEM) and DNS/IP sinkhole.

2.1 Incidents divided by category

The incidents were divided into nine categories. The classification comprises all kinds of events reported and handled by CSIRT-type teams. Categories are based on the type and consequence of the security-compromising activities, connected with the process of attack on an IT system and its use. This classification is useful mostly for operating activities aiming to solve incidents. In practice, many methods and techniques were used in the analysed incidents, as a means to accomplish a certain goal.

Incidents processed by category:

Incident category	Description and event examples
Abusive Content	Distribution of abusive and illegal content (e.g. distributing spam, distributing/sharing copyright protected materials – piracy/plagiary, child pornography) as well as offensive content/threats, and others violating the rules of the Internet network.
Malicious code	Infections and malicious software distribution (e.g. C&C hosting, malware in e-mail attachments, or links to an infected URL address).
Information gathering	Activities aiming to gather information on a system/network or their users, in order to gain unauthorized access (e.g. port scanning, wiretapping, social engineering/phishing – including sending out phishing e-mails, hosting phishing websites).
Intrusion attempts	Attempts to gain unauthorized access to a system or network (e.g. multiple unauthorized logins, attempts to compromise a system or to disturb the functioning of services by exploiting vulnerabilities).
Intrusions	Unauthorized access to a system or network, i.e. intrusion, compromising a system/breaking past security (e.g. by taking advantage of the known vulnerabilities within the system), attack on an account.
Availability	Blocking of network resources (system, data), i.a. by sending a massive amount of data, which results in denial of service (DDoS type of attacks).
Information content security	Compromising the confidentiality or integrity of information, most commonly as a result of a prior system takeover or interception of the data during transfer (e.g. interception and/or disclosure of a certain data set, destruction or modification of the data in a certain data set).
Fraud	Profiting from unauthorized use of network resources (information, systems) or their misuse (e.g. using the name of an organization without permission, using an organization's resources for non-statutory purposes).
Other	Events which don't fit into any of the listed categories

The largest group among the processed incidents was the one including the Abusive content class (26, 7%). **In comparison with the year 2017, there was a significant decline - by 22 pp. (48,9% in 2017). The second place came to the attacks on availability (23%), similar to the previous year (19,5%).** Subsequent places belong to the incidents from the information gathering group (21,6%) – here a significant increase was noted as compared with the previous year (6,9% in 2017); malicious code (18,2%) – a significant increase in comparison to the previous year (5,5% in 2017); intrusion attempts (4,4%) – a big decrease since the previous year (14,7% in 2017), fraud (3,3%) – similar to the previous year (2,9% in 2017). The least frequently occurring incidents belonged to the information content security – 2,1% (0,4% in 2017). Network intrusions consisted in less than 1%. Other kinds of incidents, not falling under any of the mentioned categories, consisted in 0,1% of all incidents.

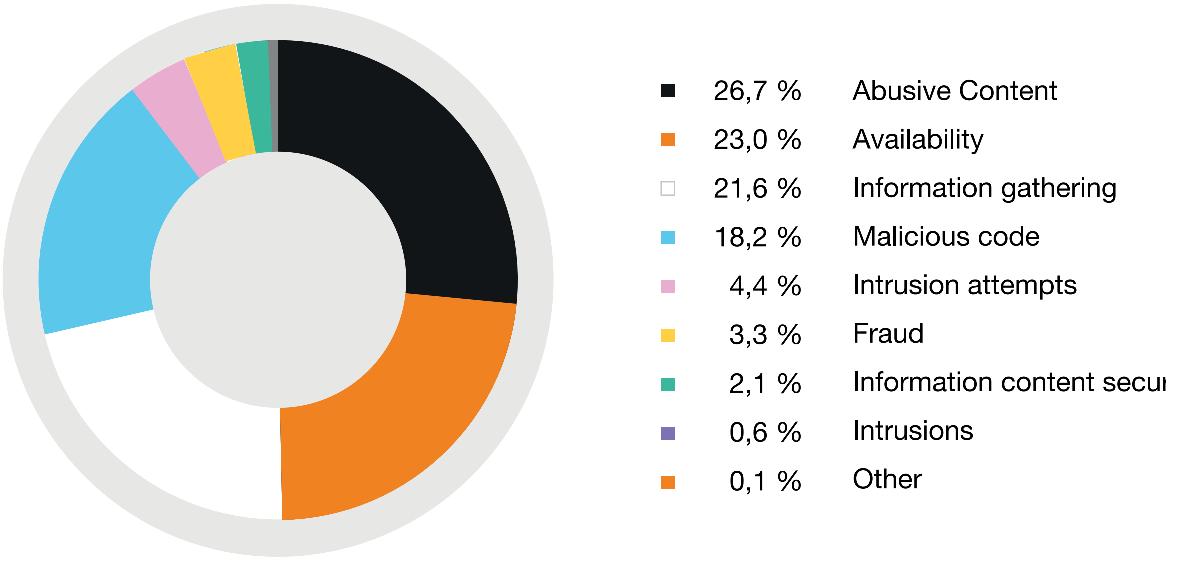


Figure 1 *Percentage distribution of incidents handled by CERT Orange Polska in 2018, divided by category.*

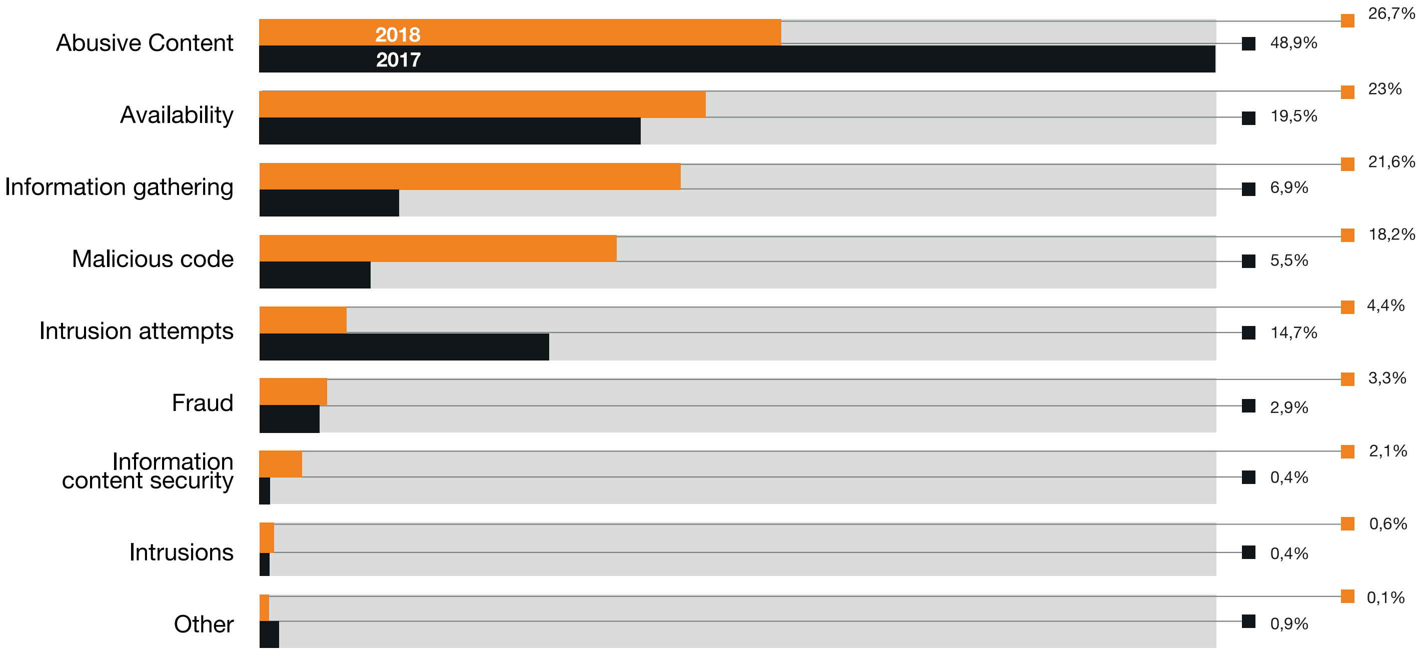


Figure 2 *Percentage distribution of incidents handled by CERT Orange Polska in 2018, divided by category, as compared with the year 2017.*

In 2018, the occurrence of incidents was not equally distributed in time. Above all, one can see a significant increase of the incidents handled in the last month of the year – meaning during the holiday period – it is then when malicious campaigns take the greatest toll. One of the methods used was phishing through sending-out fake invoices, impersonating various companies (including Orange).

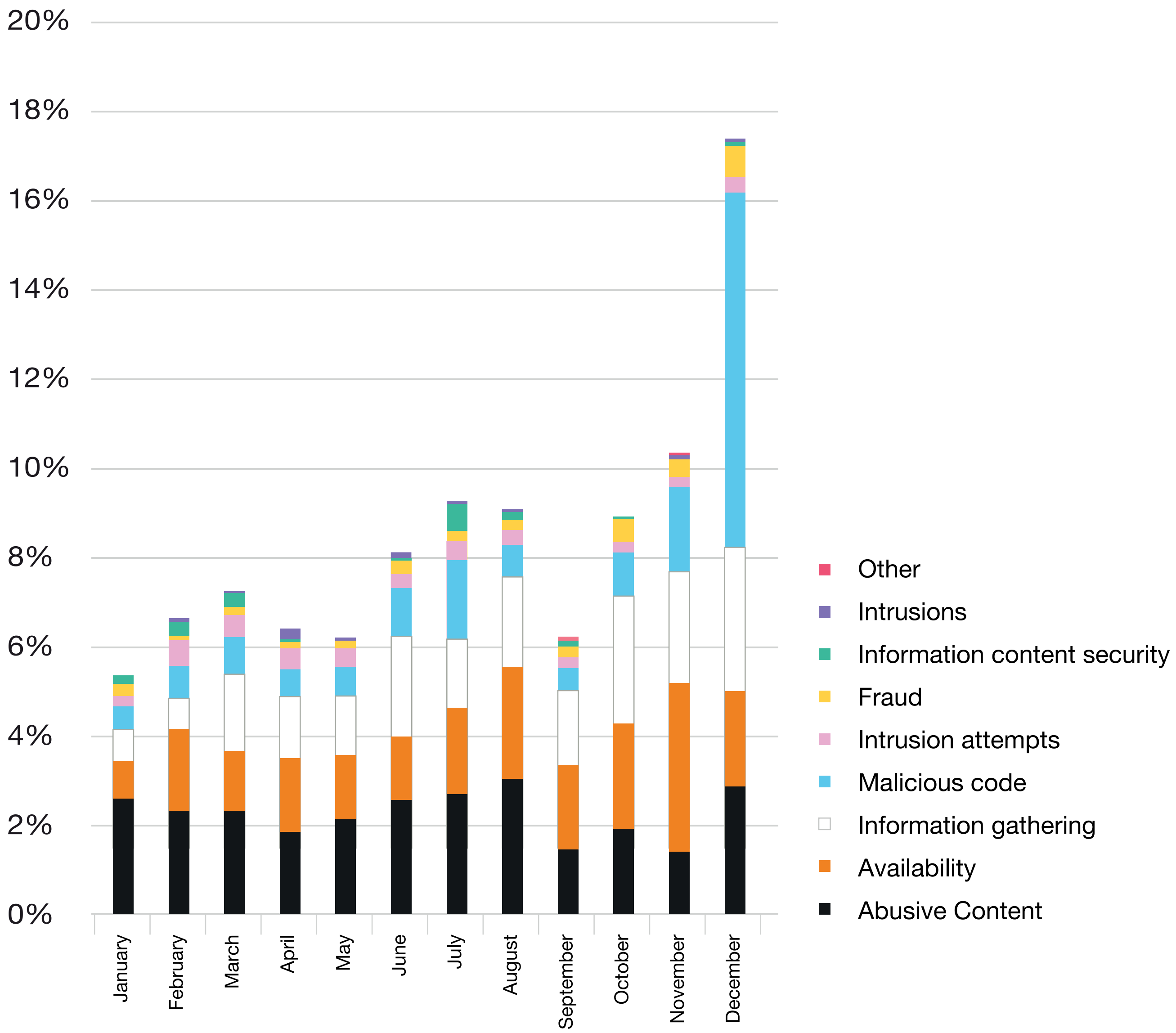


Figure 3 *Monthly distribution of incidents from 2018, divided by category.*

Abusive content

Incidents of the “Abusive content” kind were the largest group of those processed in the year 2018 (26,7%), similarly to the previous years. Among them, the cases of sending-out spam was the most numerous. Other incidents in this group were i.a. ones concerning copyright violation (e.g. piracy) and distribution of illegal content (e.g. racist content, child pornography, or inciting violence). Particular intensification of incidents from this category

Availability

The incident class called “Availability” consists mostly of Distributed Denial of Service (DDoS) type attacks. There was 6,7% incidents of this kind, and most of them were processed in November, the least in January. Just as malicious software, they may pose a serious threat and cause significant losses, which is why we have dedicated a separate section of this report to these incidents.

Information gathering

The group described as “information gathering” consists mostly of port scanning and phishing. These kinds of threats are in most cases an element of a more advanced attack, aiming for information theft or financial scam. In 2018, 21,6% of incidents from this category was noted, most of which occurred in the fourth quarter of the year.

Malicious code

The “malicious code” class of incidents consists of infections (i.a. infections with ransomware type of malware), malicious software distribution [including i.a. malware in e-mail attachments, hosting malicious websites, or hosting Command &Control servers(C&C)], remotely controlling a network of infected computers. Incidents of such characteristics consisted in 18,2% of all incidents handled in the year 2018, most of which occurred in December. This was due to an increased number of malware campaigns (malicious software as an attachment or link leading to a malicious URL), connected with fake invoices. In practice, in most of the incidents analysed, cybercriminals achieved their goals particularly because of malicious software, which is why this kind of threat has been also described in a separate section of this report.

Intrusion attempts

The “intrusion attempts” category encloses mostly efforts to bypass security through taking advantage of vulnerabilities within a system, its components, or entire networks, as well as log-in attempts onto services and access networks (password guessing), to gain access to a system or take control of it. There was 4,4% of attacks of such characteristics. The largest number of this kind of incidents was processed in February.

Fraud

The “fraud” category consists mostly in cases of unauthorized use of resources and using the name of another subject without its permission. These cases consisted in 3,3% of all incidents, and most of the incidents from this category occurred in the fourth quarter of the 2018. The reason for this was the increased number of attacks through impersonating well-known brands and institutions, including i.a. Orange, as a part of malware campaigns.

Information content security

Here, cases of unauthorized access to data, and alteration/removal of datasets can be distinguished. There was 2,1% of this kind of cases noted. Still, such incidents are of critical significance. In practice, they mean serious problems connected with data leaks or other consequences of unauthorized access to data. The largest number of these incidents was noted in July, and the lowest in November.

Intrusions

This class consists of the types synonymous with the “intrusion attempts” class, however these ones having a positive outcome for the attacker. There was 0, 6% of such attacks in the year 2018. Most of incidents from this category were processed in April.

Other

Incidents not classified in any of the previously mentioned categories consisted in as little as 0,1% of all cases. No dominant kind of incident can be distinguished within this group.

”

The largest group among the processed incidents was the one including the abusive content class

26,7%.

3. Overview of the most important events and threats in Poland and around the world in the year 2018

January

World

Meltdown and Spectre - discovery of the attack

Discovery of the security gaps Meltdown and Spectre in Intel, AMD, and ARM processors. The gaps allow programs to steal the data processed on a computer through reading the memory of other programs. The malicious program using the Meltdown and Spectre vulnerabilities on personal computers, mobile devices and cloud, also allows to intercept authorization data.

Poland

Malicious messages on Facebook

Facebook and Messenger users were receiving malicious messages from compromised accounts of their friends, saying that they would find their altered photos under the link. Opening the link made it possible to steal logins and passwords from Facebook, or enabling a premium SMS service on the phone.

Orange

Fake e-mails impersonating Amazon

The CERT Orange Polska team identified and analysed a phishing campaign impersonating the Amazon store. The experts revealed that it was an attempt to steal logins and passwords.

February

World

Taking over computers as a means of obtaining cryptocurrencies

Around 4 thousand websites, including ones belonging to government institutions of Great Britain, USA and Australia were used by an external plug-in used for getting access to a website. The visitors became victims of the so-called cryptojacking, where the computing power of processors is used to get cryptocurrencies.

Poland

Data leak from a government website

One of the websites launched by the Ministry of Finance made it possible to see the personal data of people who were supposed to receive a PIT tax rebate. Among the data, there were i.a. social security number and taxpayer identification number.

Luty

Poland

Text messages impersonating unpaid bills

A text message named “invoice” contained a debt notice. A link in the message redirected to a fake DotPay page upon opening in an attempt to extort money.

Orange

Phishing impersonating Orange

Internet users were receiving fake e-mails impersonating the @orange.pl. domain

Marzec

World

Data of 1,1 billion Hindi people sold for 6 pounds

A leak of financial and personal data from the national database of India (Aahaar), storing the data of over a billion Indian citizens. Anyone could download it. The data includes i.a. biometrical data, fingerprints, retinal scans, and photographs.

Poland

The Thomas Case

After 6 years of criminal activity, Tomasz T. (alias Thomas, ArmagedOn) is arrested by the police. The cybercriminal is known z from dozens of attacks aimed at Polish internet users. Using e-mail campaigns, he was infecting their working stations with malware. He was impersonating i.a. Allegro, PayPal, and DotPay.

Orange

The activity of the QuantPro malware in the Orange network

CERT Orange Polska team noted the activity of the QuantPro malware. The conducted analysis suggested that the infections affected around 1500 users. The analysis can be found on cert.orange.pl website.

April

Poland

New phishing campaign “sales blocked”

The attack was aimed at the users of the Allegro service, and consisted in sending out e-mails informing that the user’s sales have been blocked. The e-mails contained a link to payment of a minor invoice in order to unlock the account. The messages looked realistic enough for the users to open the link without suspicion.

Poland

Free Biedronka coupons

A fake website made in the likeness of the Biedronka store’s site, offered vouchers worth 50 PLN, which could be bought at an attractive price. Customers tempted by that offer were being redirected to a page impersonating DotPay upon clicking on the banner. As a result, filling the payment data allowed the cybercriminals to steal money from Polish people’s bank accounts.

May

Poland

Messages impersonating Alior Bank

Mailing campaign aimed at Alior Bank customers. The messages included information about the possibility of getting a voucher by clicking onto the attached link. Opening the link caused an infected file named "Invoice.doc" to be downloaded.

Poland/UE

GDPR – important changes in personal data protection

On the 25th of May, the GDPR act came into force. It applies to Poland, and all other countries belonging to the UE. The regulations aim to enforce the law in terms of personal data protection, applying to all subjects, both public and private, which process personal data.

Orange

Orange "lotteries"

While browsing the internet, the users could encounter a pop-up window or a tab saying: "Dear user, congratulations!". The contents suggested that Orange allegedly gives out Samsung Galaxy smartphones. To receive one of them, one had to fill a fake survey, giving one's data, including login and password.

Orange Polska and NASK hosts the prestigious meeting of European CSIRTs

On 24 and 25 May cybersecurity specialists from Europe met at Orange Polska head-quarters. This was one of the three annual meetings organized as part of the TF-CSIRT "Trusted Introducer" initiative, which brings together leading European teams to respond to IT security threats.

June

World

Rogue Chrome extension

An extension named "Desbloquear Conteúdo" appeared in the Chrome Web Store, which upon being added to a browser conducted a man-in-the-middle attack as a means to get payment data. As the user tried to log into his or her bank account, a hostile script extracted certain information, such as login, password, and one-time security code.

Poland

Personal and payment data leak affecting Ticketmaster company customers

Customers of the Ticketmaster company were put at the risk of leak of their personal data in the period between February and June. All music fans who bought, or attempted to buy tickets could have lost personal, as well as payment data.

Poland

Mailing campaign with Mundial tickets

In June, right before the Mundial 2018, internet users were receiving e-mails informing them that they have just won tickets to the World Championship. To claim the prize, one had to click on a link or open a malicious attachment in .pdf or .doc format. The next step was filling contact and payment data, and paying a small fee. Internet users following these instructions lost their money, and never received the tickets.

July

World

Error in the Samsung brand smartphones

Owners of the new Samsung Galaxy smartphones were unintentionally sending out photos to random people from their contact list. The problem was caused by the Samsung Messages application, which would send out pictures from the phone's storage without permission. Moreover, there was no telling to whom the pictures were sent to. The users were informed about the situation by the people who received their photos.

July

Poland

Fake sale on the neo24.pl store

The customers of Neonet received a text message of a 30% sale of all the products in the web store. The sale, however, did not concern the official Neonet website, but rather the mistrzostwa.neo24.pl website created by the cybercriminals. The fake store coerced some customers, and charged their accounts. The purchased goods were never sent, though.

Orange

Fake DNS incidents

CERT Orange Polska noted even two million events a day, connected with Fake DNS. The attack consisted in swapping DNS server names in network devices, or directly in the browser.

August

World

Deeplocker - how artificial intelligence creates malware

During the Black Hat USA conference, the IBM company presented a new kind of malware named Deeplocker. The malicious software uses artificial intelligence technology, which provides immunity to the so-called reverse engineering.

World

DDoS attack on the central bank of Spain

The central bank of Spain was cut off from the Internet through a successful DDoS attack. The attack deprived the customers of access to the bank's website, but as the bank assured, financial operations did not suffer.

Poland

Fake BZWBK ap-plication

Customers of the BZWBK bank were put at risk of us-ing a fake "BZWBKlight" application available at the Play Store. The application's purpose was to extort in-formation. It has probably also allowed to access messages, send premium text messages, and intercept bank access codes.

Poland

Act on the National Cybersecurity System

The act on the National Cybersecurity system came into force on 5th of July 2018. It is the first document regulation the matter of cybersecurity in Poland. The act concerns i.a. operators and providers of the key services, competent bodies responsible for cybersecurity, and it establishes three national computer incident reaction teams.

Orange

Malicious applications in the Android System

CERT Orange Polska noted activity of the Bankbot.Anubis malware in a mobile network, the activity of which reached 41%. The software disguised itself as a harmless application available for devices with the Android system, and it aimed to coerce the user into grant it additional privileges connected with accessibility service. It allowed i.a. theft of logins and passwords to bank accounts.

September

World

Facebook – Data theft from 30 million accounts

Around 30 million Facebook accounts were hacked. This was done with the use of the “view as” function, which allowed the hackers to view information. The users lost personal and contact data, including phone numbers, e-mail addresses, and all other information available on the Facebook platform.

World

Data theft from British Airlines payment cards

Customers, who attempted to book flight tickets in the British Airways since 21st of August, were at risk of losing personal and financial data from their payment cards. The cybercriminals took advantage of security gaps on the airways’ website, as well as in the mobile application.

Orange

CyberTarcza detects over three thousand Bitcoin Miner infections

The Orange CyberTarcza noted 3143 infections using Bitcoin Miner, software which uses a machine’s computing power to mine cryptocurrencies. The user is often unaware of the software being installed on his or her computer.

October

World

Google+ is shut down after a hacker attack

A security vulnerability allowed hackers to gain access to the data of over 500 thousand Google+ users. Google decided to shut the social network down. Google+ will be shut down soon for private users.

Poland

Fake discount code at OLX

Criminals offering products at an attractive price at OLX coerced potential buyers into buying through pseudo online stores. The messages included a discount code to purchase a product at a lower price. This way, the fake stores extorted money for items which they would never send.

Poland

Malicious e-mails with an invoice from Trusted Profile

Cybercriminals were sending out malicious e-mails impersonating Trusted Profile. The title of such message suggested an invoice, whereas the content concerned verification of the Trusted Profile through clicking on a link, which resulted in downloading an .exe file and infection of the computer.

November

World

Data theft from the Marriott hotel chain

The international Marriott hotel chain, announced a massive data security breach in the Starwood reservations database. The data leak concerned around 500 million guests from various hotel chains, such as Sheraton, Westin, Le Meridien, Aloft, The Luxury Collection and W Hotels. The cybercriminals have probably already gained access to the database in the year 2014.

World

Infected games on Google Play - over 500 000 us-ers downloads malware

Google Play offered a download of 13 mobile games along with malicious software. Over 500 thousand downloads were noted. The malicious applications were positively verified by Play Protect.

Poland

False SMS alert from RCB

The citizens of the Dukla and Horodlo municipalities, which lay near the Ukrainian border, received fake text messages from Alert RCB, concerning military con-scription of the men, and the necessity of appearing in the municipal office due to the critical situation in Ukraine. The national Security Centre denied this in-formation, and passed the issue to the ABW and Police.

Orange

Modems sending malicious text messages

CERT Orange Polska identified malicious text messages containing information about a rebate, which was possible to get by clicking the provided link, and filling a form. The messages were prepared in English and Italian. They were aimed at the users located in Great Britain and Italy. The numbers used for this were Polish, from devices using a SIM card.

December

Poland

Data leak from morele.net

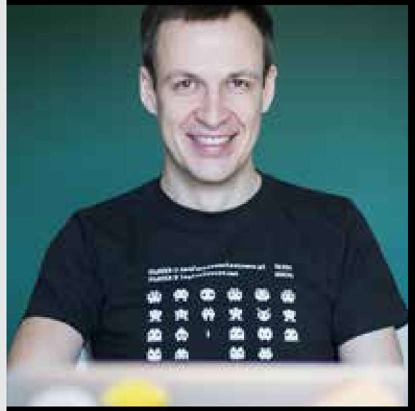
Data of over 2 million customers of the morele.pl store was stolen. The hackers also managed to steal the data of customers who had already closed their accounts on morele.pl, and which should no longer be stored in the company’s servers.

Poland

Nomination of the National Cybersecurity Executive

On the 7th of December, the Prime Minister nominated the National Cybersecurity Executive. The executive plays the most important role in the national security system. He is responsible for coordination of operations and enforcement of the government’s policy in the field of ensuring cybersecurity.

Partner's Commentary



Adam Haertle,

Renowned speaker, trainer and lecturer. Since the year 2004 he regularly performs at all significant conferences dedicated to security in Poland, where he receives the highest ratings in participant surveys. Lecturer of two postgraduate courses at SGH and Bialystok University of Technology. In 2017 he gave over 70 lectures dedicated to the matters of web security, threats of using electronic banking, privacy and data protection in businesses, both for open and closed audiences all across the country. In his lectures, he describes real threats awaiting businesses and users, using simple language and real-life examples. He deals with security professionally since over dozen of years, first in the Deloitte company, and later in UPC, where for 12 years he was responsible for all matters regarding data protection in the country and region. Since six years he runs the ZaufanaTrzeciaStrona.pl website, one of the largest Polish web pages dedicated to cybersecurity.

One trend always comes true in all reports and in all forecasts – the number of attacks and their victims will continue to increase. Their proportions are changing, the methods of criminals are evolving, some attacker groups are disappearing and others are replacing them, but the losses from attacks have been and will be a permanent element of our landscape.

The market of products designed to provide us with security online is also growing incessantly. An increasing number of boxes are analysing traffic and eliminating attacks and new generations of security specialists continue to appear in the market, but this still does not eliminate the problem and it does not appear that the situation is likely to change diametrically in the near future. What lies at the heart of this phenomenon? In my opinion, it is the human nature.

"The problem lies between the chair and the keyboard," is a popular saying among IT specialists that demonstrates their attitude toward system users. Most people in charge of security believe that if a user has clicked on an attachment and infected their computer, the problem lies with the user, as "they could have chosen not to click". I have never heard a security specialist say after such an incident "we have to think about how to prevent any harm from coming to a user even if they do click". Because a user will click. If not this one, then another one will. If not today, then tomorrow. Sometimes even during a training course that is meant to teach them not to click. Unfortunately, very few companies build their security strategies around that assumption. Such tilting at windmills does not lead to any good results – because users do click; we may just learn about it too late.

At a recent large conference, when I asked a room full of security specialists who monitors the execution of PowerShell scripts outside of the IT Department, a dozen people from among the hundreds present in the room raised their hands. Such monitoring is not difficult to implement and can be very useful – it can identify not only attacks, but also the Accountancy Department employees who should transfer to the IT Department. When I asked who had prevented users from being able to execute VBS and JS scripts on workstations, someone blurted out "that's impossible". When I asked whether they had even tried, they responded negatively.

It is time to change the approach to security problems. It is time to stop blaming users whose responsibility is to read their mail for clicking on their e-mails. It is time to ponder what kind of simple changes in the configuration and monitoring of workstations can limit the number and effects of incidents – without the users' knowledge and participation in that process. After all, we are the experts and it is us that bear the responsibility to protect those who cannot see to their own security.

"It is time to change the approach to security problems. It is time to stop blaming users whose responsibility is to read their mail for clicking on their e-mails. It is time to ponder what kind of simple changes in the configuration and monitoring of workstations can limit the number and effects of incidents – without the users' knowledge and participation in that process.

3.1. Volumetric attacks on infrastructure – DDoS

Distributed Denial of Service (DDoS) attacks are one of the simplest and most common attacks on networks and computer systems, and yet one of the more dangerous in consequences. Their main purpose is disturbing or preventing the use of services offered by the affected network service system, which results in the victim's infrastructure being paralyzed through mass sending of queries to the targeted service.

3.1.1. DDoS Attacks – traffic characteristics

Below we present traffic characteristics of UDP protocol ports most commonly used in DDoS attacks, on the analysed Orange Polska connections. The data presented on the charts is averaged.

Port 389 is used by the LDAP (Lightweight Directory Access Protocol) service, used for accessing directory services. **The highest traffic on this port (over 50 Gbps) on the analysed Orange Polska connection was observed in March and November.**

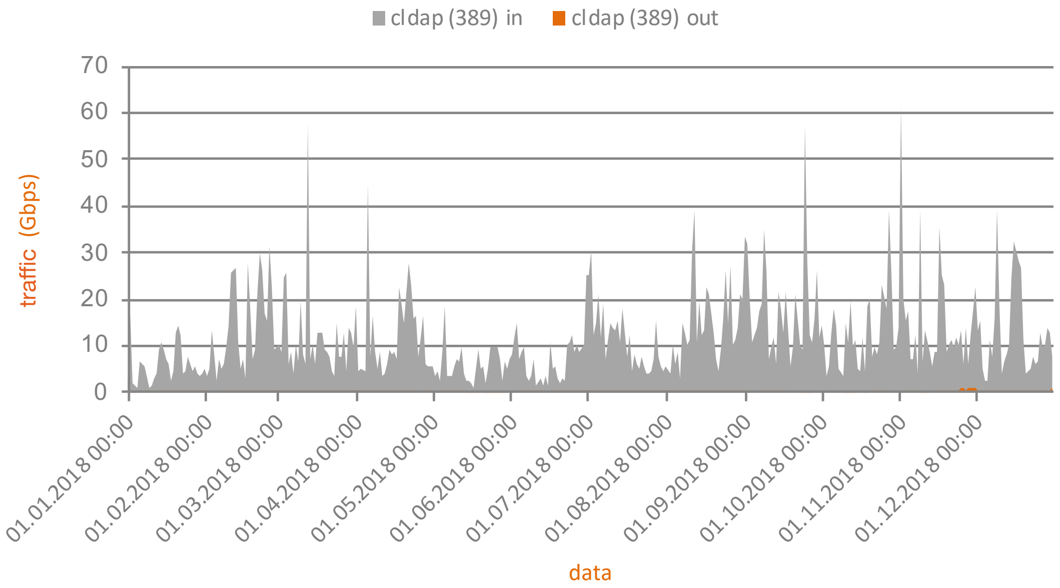


Figure 4 *Traffic characteristics on port 389 on the analysed Orange Polska connection.*

Port 123 is used by the NTP protocol (Network Time Protocol) service used for synchronizing time in IT and telecommunications systems. **The highest traffic on this port (over 14 Gbps) was observed in November.**

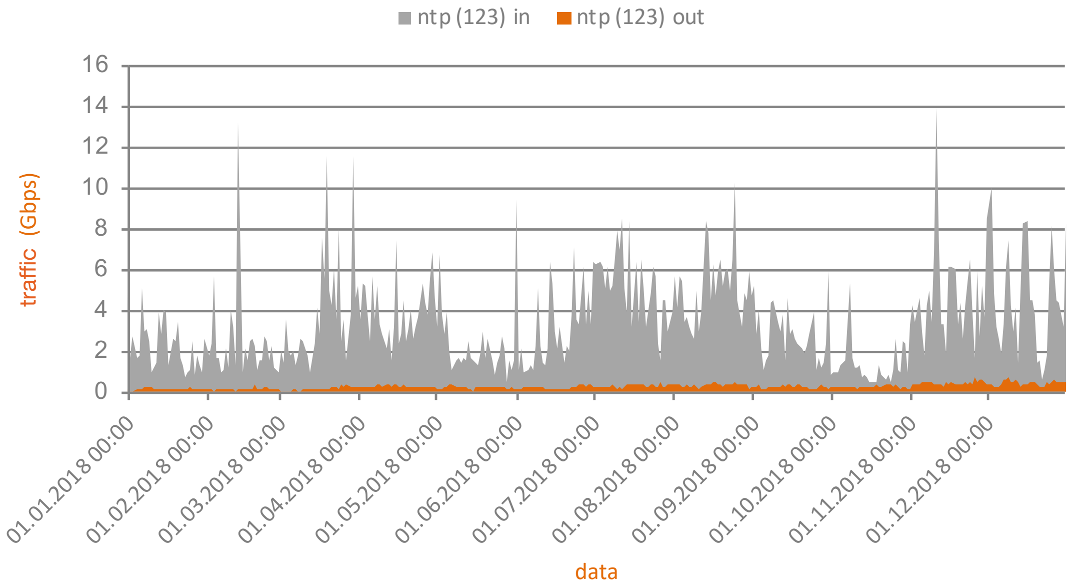


Figure 5 *Traffic characteristics on port 123 on the analysed Orange Polska connection.*

Port 53 is used by the DNS (Domain Name System) service, responsible for mutual translation of domain names and IP addresses. **The highest traffic on this port (over 30 Gbps) was identified in January.**

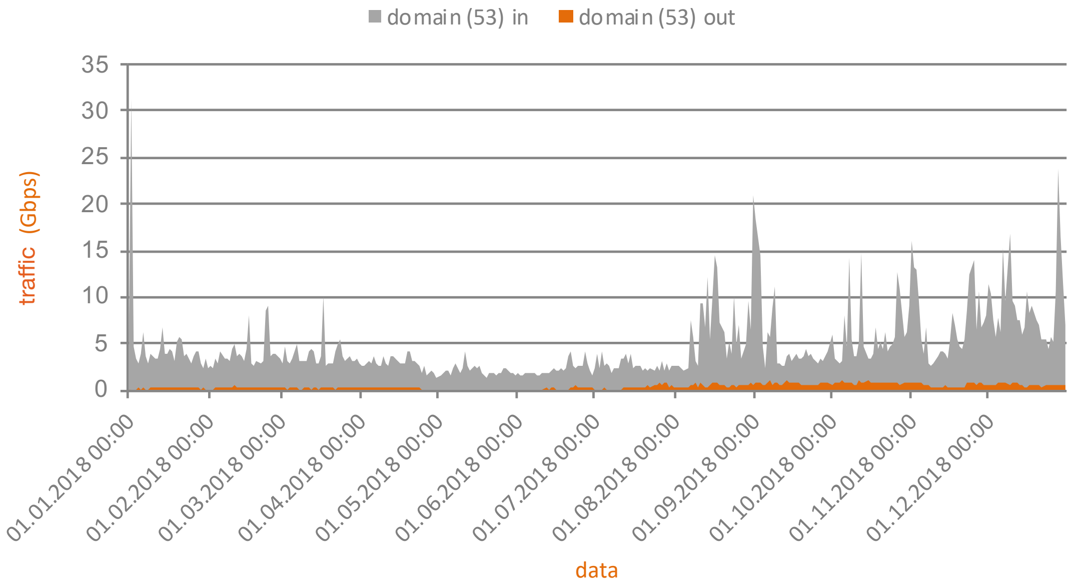


Figure 6 *Traffic characteristics on port 53 on the analysed Orange Polska connection.*

Port 1900 is used by the SSDP protocol (Simple Service Discovery Protocol), which is used for detecting UPnP (Universal Plug and Play) devices e.g. keyboards, printer, or routers. The highest traffic on this port (over 12 Gbps) was observed in March.

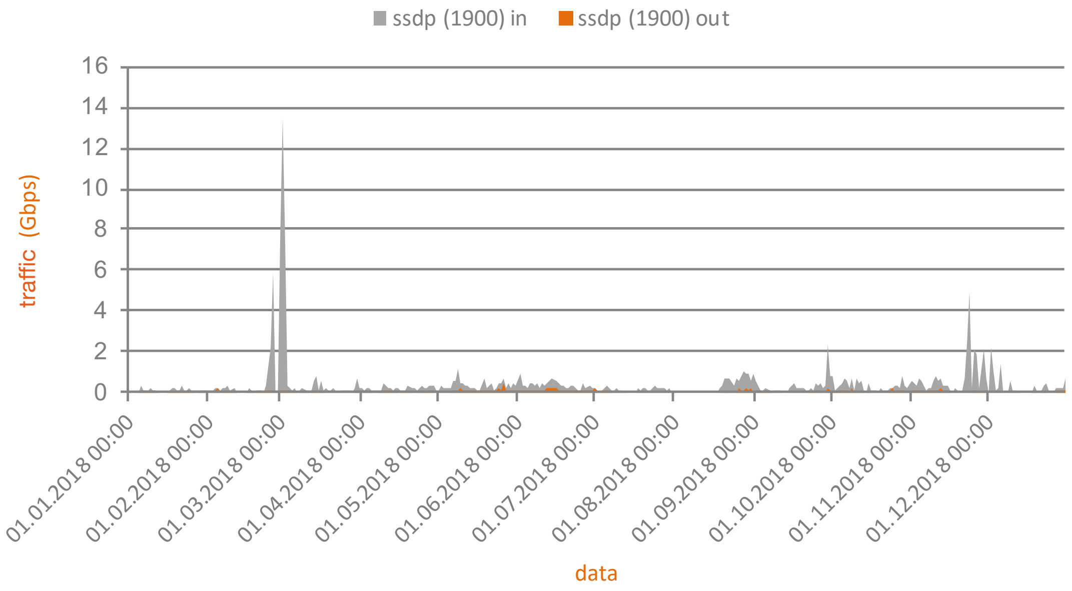


Figure 7 *Traffic characteristics on port 1900 on the analysed Orange Polska connection.*

Port 19, used by the CharGen protocol (Character Generator Protocol), which is used for generating signs for test purposes. The highest traffic on this port (over 3 Gbps) was observed in July.

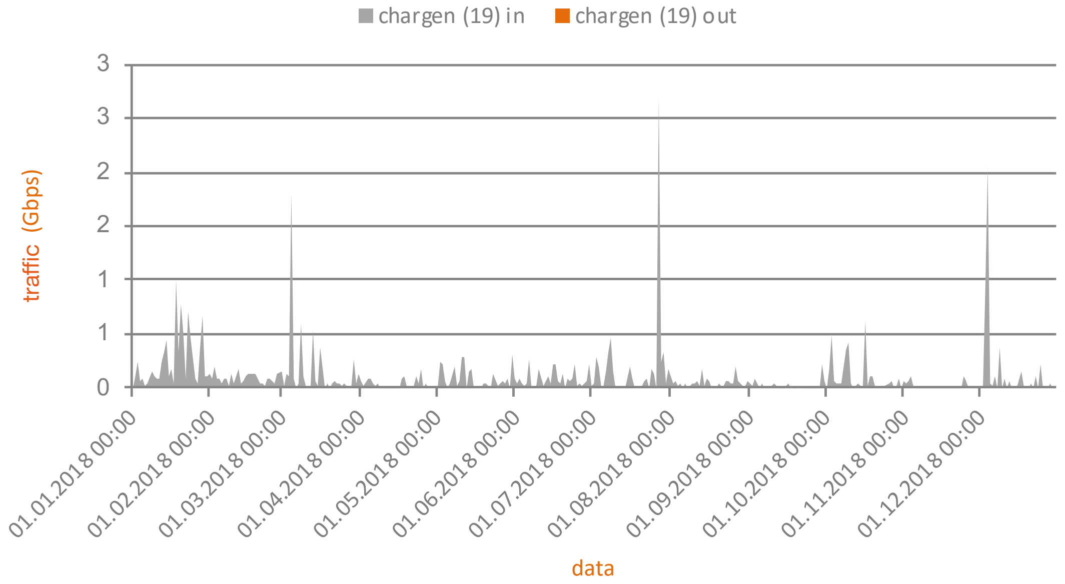


Figure 8 *Traffic characteristics on port 19 on the analysed Orange Polska connection.*

3.1.2 DDoS Attacks – types of attacks

The DDoS attack classification used by CERT Orange Polska is based on three categories of severity. This aspect is dependent on traffic volume and duration time of the anomaly. High alert usually has significant influence on availability of the service, while the average and low ones limit the service only under certain circumstances.
The frequency of DDoS attacks over the course of last few years remains toughly the same, although a little more of them was registered in the year 2018 as compared to 2017. **The highest number of alerts from the year 2018 was registered on 2nd of July (over 430) and 2nd of December (over 420).**

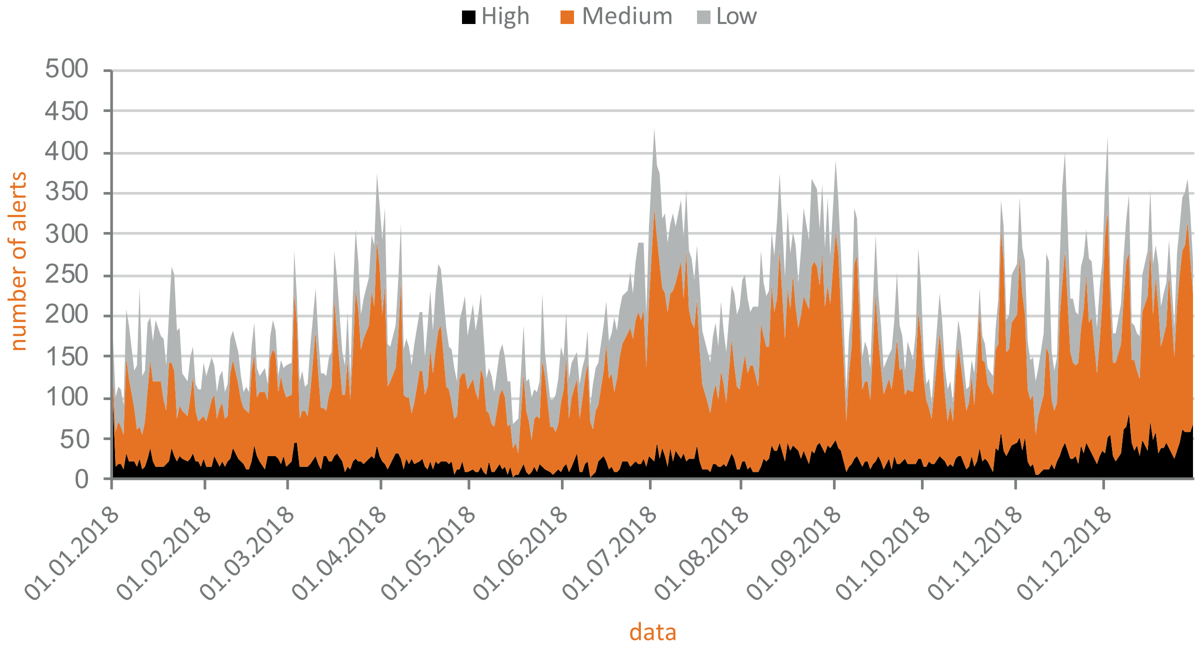


Figure 9 *DDoS alert distribution divided by their severity.*

The highest share in the percentage distribution of DDoS attack severity consists of the ones of average severity – more than a half of all noted events. In comparison with 2017, there is 11% more of them.
As in the previous years, the smallest share consists of attacks of the highest severity. It amounts to 12% in the year 2018 and 20% in 2017.

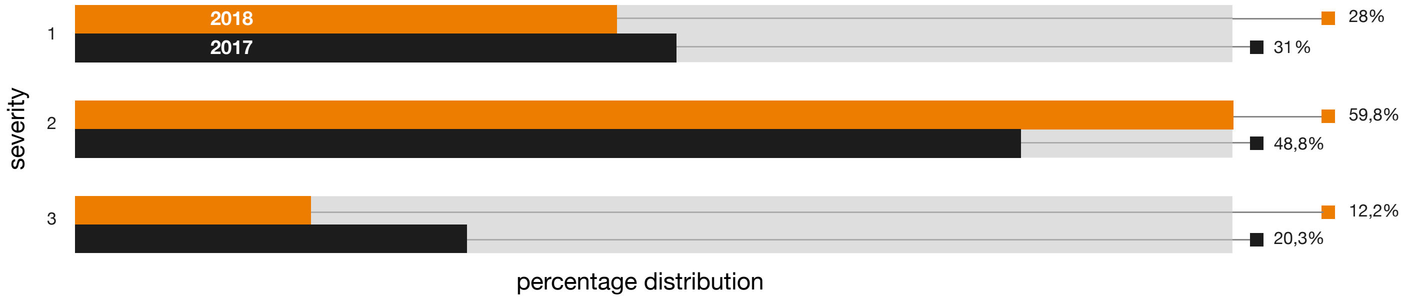


Figure 10 *Percentage distribution of DDoS attacks severity.*

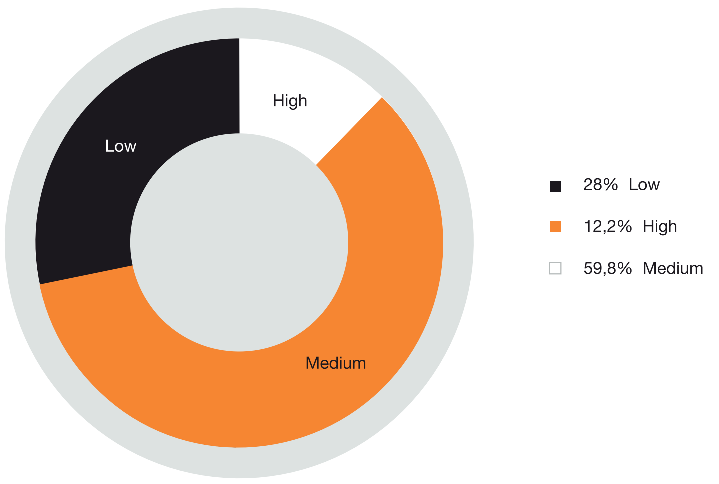


Figure 11 *Chart showing the severity of DDoS alerts in percentage distribution.*

In the distribution, as in the previous years, the most frequently occurring volumetric attacks were, alongside UDP Fragmentation, Reflected DDoS attacks using UDP (CLDAP, DNS, NTP, SSDP, CHARGEN) protocols. **Among them, the most commonly used were open LDAP servers – identified in 30% of all attacks (the highest increase in comparison with the year 2017, by almost 2%)**, wrongly configured time servers (NTP) – identified in 22% of all attacks (12% in 2017), open DNS servers (21%), and the CHARGEN protocol (3%) as well as SSDP (1%). UDP Fragmentation attacks were identified in over 60% of all attacks, 55% in 2017.

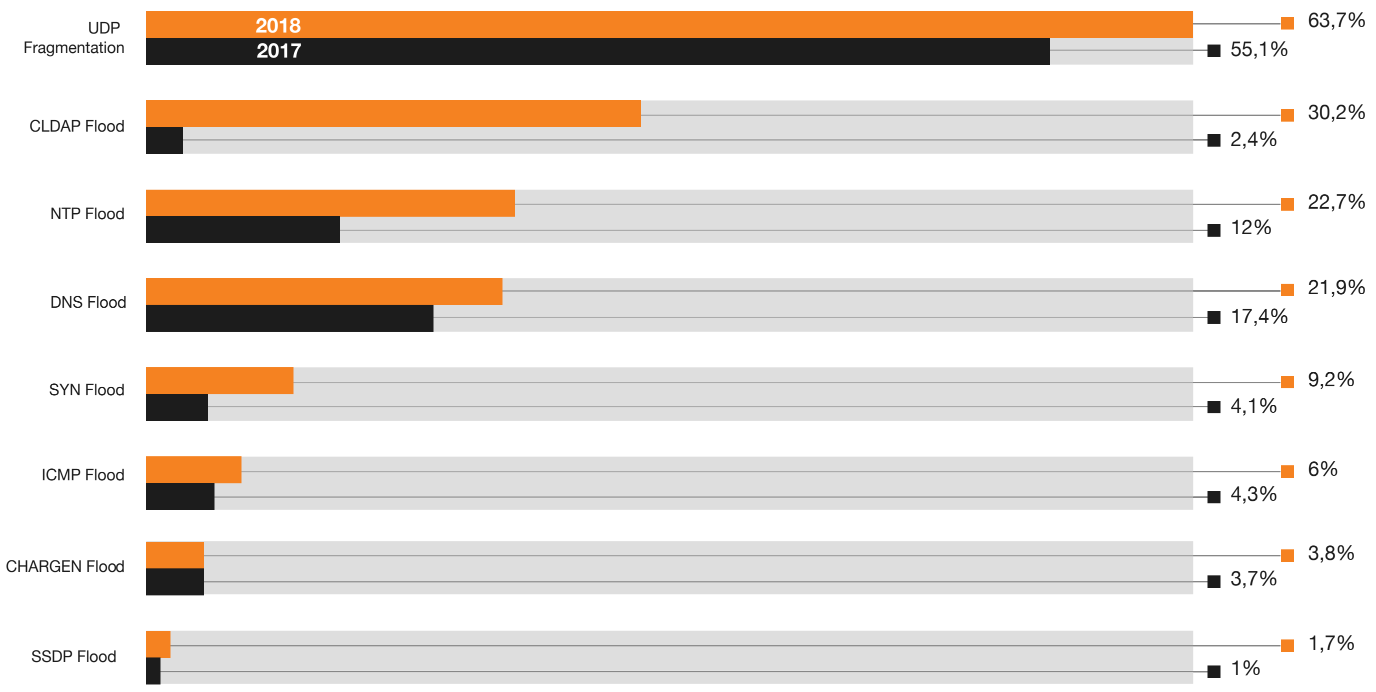


Figure 12 *The most common types of DDoS attacks.*

Attack type descriptions:

UDP Fragmentation – – an attack consisting in sending large UDP packages by the adversary (above 1500 bytes). Bearing in mind the necessity of reconnecting defragmented packages on the end device, the use of additional processor resources is necessary, which burden the computer's system.

Reflected DNS – called a reflected attack, meaning a method of using vulnerabilities in network communication protocols. Vulnerabilities in protocols such as UDP, DNS, NTP, CHARGEN or CLDAP (Connectless Lightweight Directory Access Protocol) can be used for amplification.

ICMP Flood – a method consisting in sending a non-standard amount of large ICMP packages as a means of "flooding" the victim's computer network. Usually a network of intercepted devices (bots) is used for this kind of attack. As a result of such operation, the network capacity becomes overwhelmed, and services are blocked.

SYN Flood – attack based on vulnerability of three-way handshake, a procedure of establishing a connection used in the TCP protocol. The attacker sends a SYN flag to the ports, which is meant to initiate a connection between the source and target host. Then, the attacker's system responds with a SYN-ACK message, which opens the port and waits for connection confirmation – waits for an ACK flag from the attacker. The flag, however, is never sent, and thus the connection is never established, but for a certain amount of time, the "victim" is waiting for the confirmation, which consumes resources.

3.1.3 DDoS Attacks – attack volume and duration time

The average volume of a DDoS attack at its peak intensity observed in the Orange Polska network reached a level of 2, 1 Gbps, much higher as compared to the year 2017 (over 1, 2 Gbps). Then, **the highest observed value of traffic intensity at the peak of the attack reached around 198 Gbps/20 Mpps (82 Gbps/20 Mpps in 2017**). The increase in the force of attacks wasn't caused only by faster internet connections, but also attractive prices of DDoS attacks on the black market, as well as the use of reflective amplification and botnets based on Internet of Things devices. The percentage distribution of attack volumes is similar as in the previous years. As compared to the year 2017, there was a 6% increase in attacks between 0,5-2 Gbps, 5% increase in attacks above 10 Gbps, and a minor increase in attacks between 5-10 Gbps. In other groups, there was a minor drop in the share of attacks.

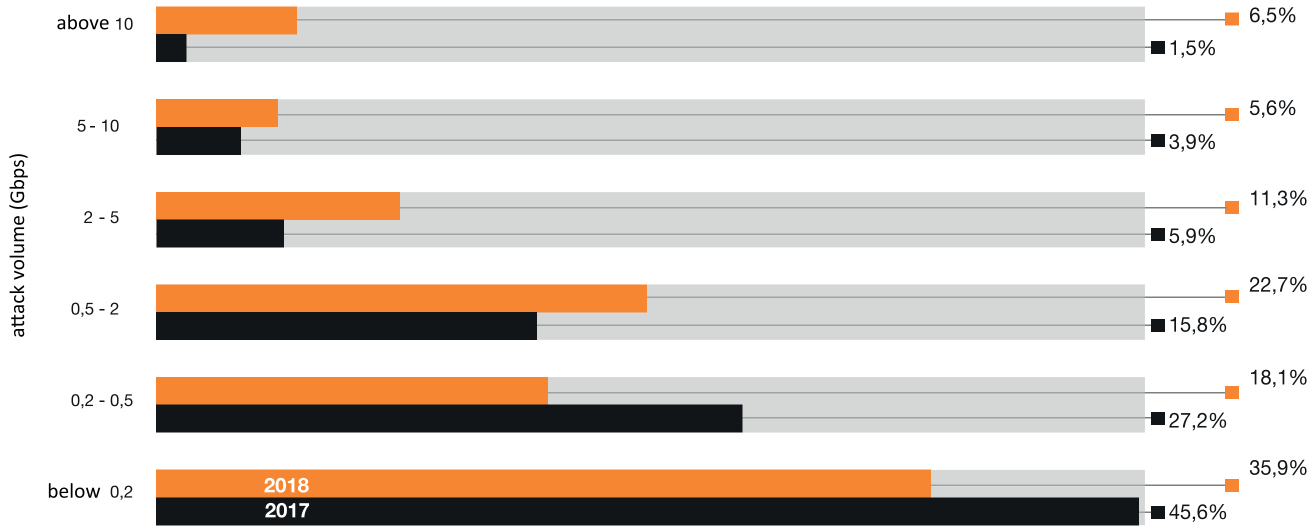


Figure 13 *Volume of DDoS attacks observed in the network.*

Similar as in previous years, a trend prevails indicating that the duration time of attacks becomes shorter. Most of the registered alerts lasted less than 10 minutes (almost 88% in 2018, a little over 72% in 2017) – an increase of 15% in 2018. In other groups, there was a minor drop in the share of attacks.
The average duration time of all registered alerts amounted to around 11 minutes (15 minutes in 2017)

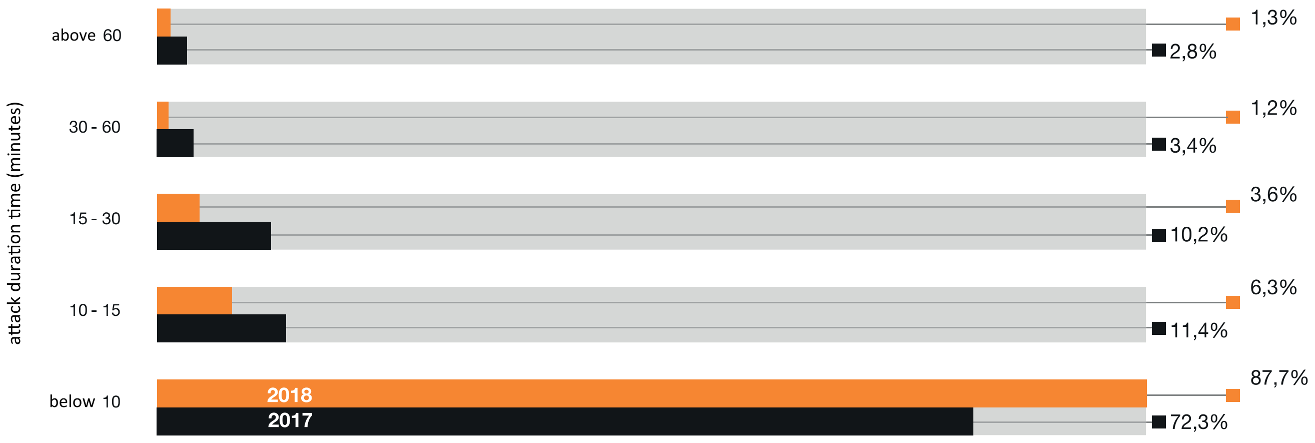


Figure 14 *Duration time of DDoS attacks observed in the Orange Polska network.*

3.2 Malicious software – selected issues

TOP3 – Trojan/PUP/Adware

In terms of quantity, the year 2018 did not stand out as compared with the previous years, almost perfectly matching our predictions concerning the evolution of malicious software. Still, the top of the list (TOP3) list occupied by threats broadly classified as Trojans, harmful and potentially harmful and unwanted applications (PUP) and more or less "aggressive" adware, which together consisted in over 80% of blocked infection attempts and installations in the systems of our users and customers. It is worth mentioning here that malicious software from this group is oftentimes very advanced, and due to various programming "tricks" applied by its creators poses a significant challenge to antivirus labs both in terms of detection, and deletion from the affected systems.

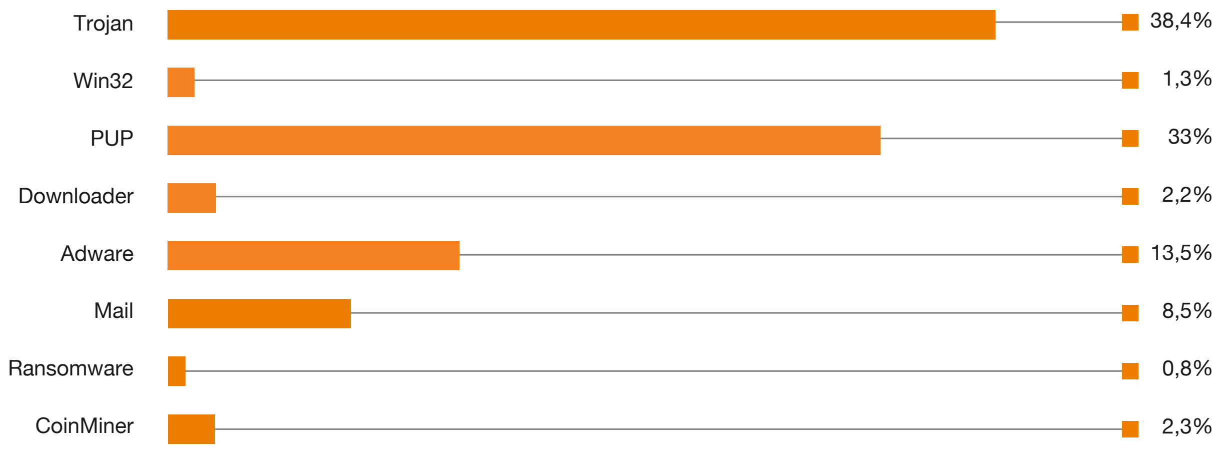


Figure 15 *2018 – main theats (%).*

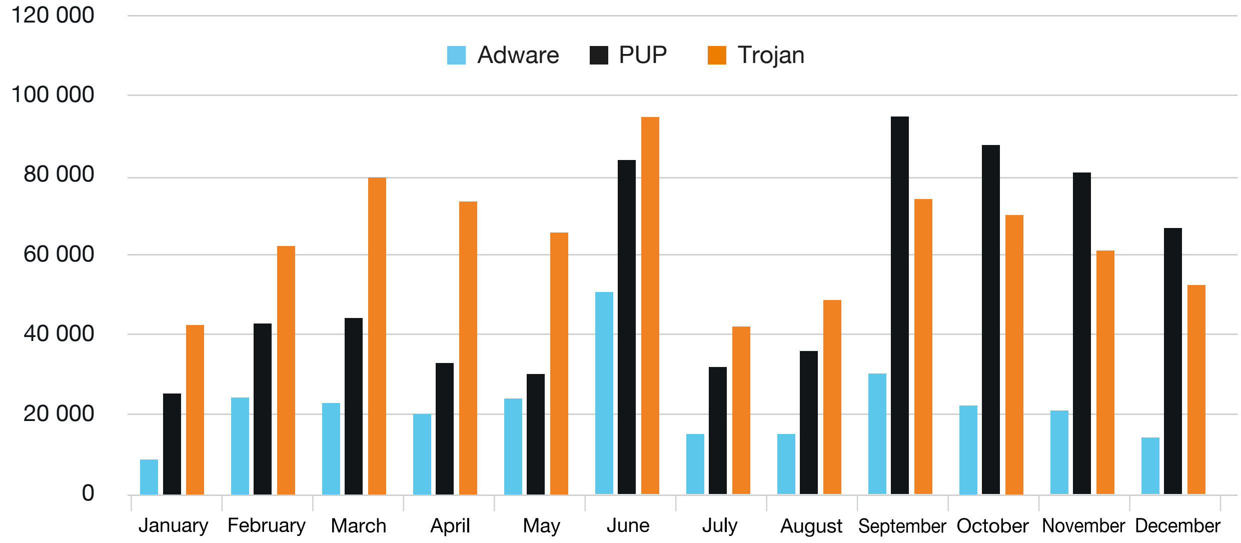


Figure 16 *TOP3, the number of infections blocked – Trojan/Adware/PUP.*

CoinMiner/Ransomware

What was interesting in the year 2018, actually happened beyond the TOP3 mentioned above (Trojans/PUP/Adware). As we anticipated, in terms of quality, technology and the media, the year 2018 belonged to cryptocurrency miners and data encrypting threats (with an emphasis on the miners). The first quarter of the year was marked by a rapid increase in the number of infection attempts with cryptocurrency mining applications. Still, antivirus labs managed to implement detection and deletion mechanisms for this kind of threats relatively quickly, which is reflected in the decrease in the number of detected miners since the beginning of the second quarter. Simultaneously, the end of the year brought a minor, but noticeable increase in data encryption attempts, which may indicate a "counterattack" of Cryptolocker and Ransomware type of threats (which can already be seen in the statistics from the beginning of 2019). However, we do not anticipate any more of the spectacular epidemics in this field.

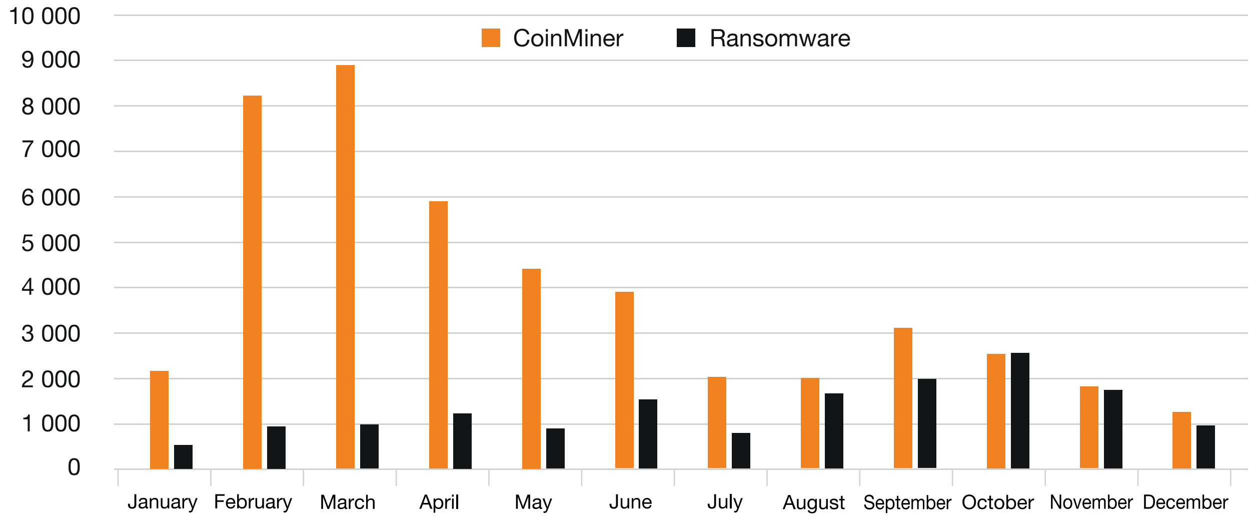


Figure 17 *The number of CoinMiner and Ransomware threats blocked in individual months in 2018.*

Electronic mail

The unquestionably most popular vector of attack in the year 2018 was electronic mail. The diversity in the message structure used by the cybercriminals presented a significant challenge for the mechanisms of detection. Attachments in different formats, links in the contents leading to infected websites, data extorting forms – all of these elements enclosed in more or less successful social engineering methods were supposed to coerce the victim to download and run the harmful scripts or applications (usually installing cryptocurrency miners, encrypting data, or viewing advertisements). The high threshold of blocked messages in the first quarter of the year, remained at a steady level until the end of the year (with a noticeable fall during the holiday season, of course).

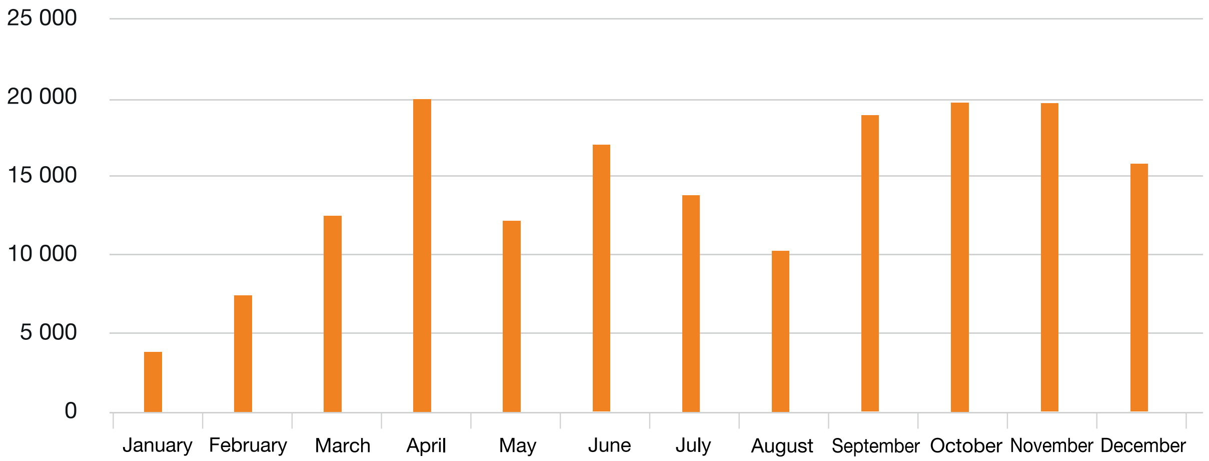


Figure 18 *The number of e-mails with malicious content blocked in individual months in 2018.*

Classical viruses

In every report, we also mention classical viruses (mostly Win32.Sality, Win32.Virut and Win32.Brontok), which despite belonging to a bygone era, are still being detected in our users' resources. This is the so-called "bottom drawer effect" or, "Oh, an old pendrive! I'll see what's on it!" Attempts to restore such old resources from the times when detection of certain types of threats was not yet at 100%, still results in several thousand blockades a month.

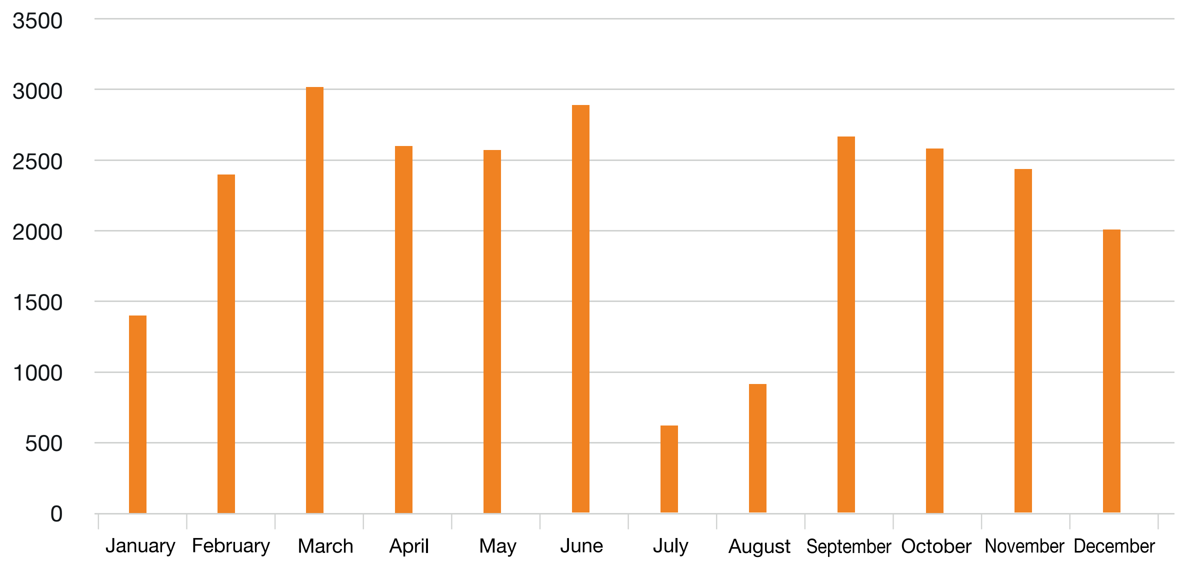


Figure 21 *The number of classical viruses blocked in individual months of 2018*

Android

Mobile threats. Their number grows constantly, which finds reflection in our comparisons. SMS-sending, ad viewing, and spying applications are the most commonly blocked/detected threats on mobile devices. What's interesting, as opposed to other kinds of threats, the comparison for the Android system shows a significant increase in detections during the holiday season.

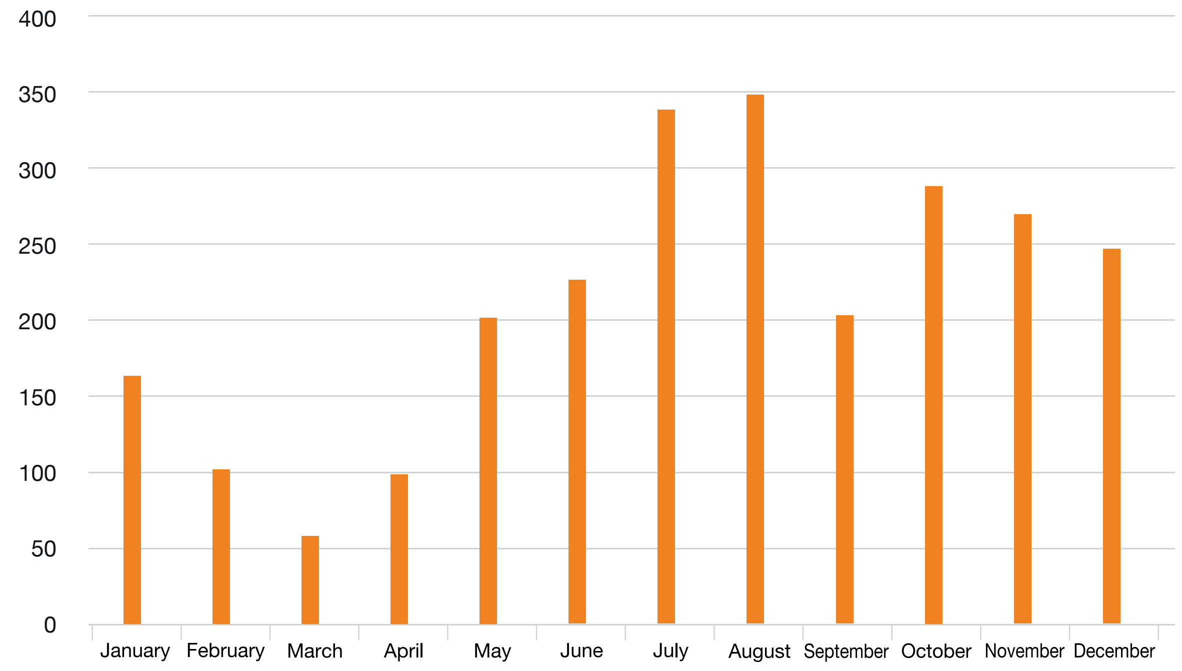


Figure 20 *The number of threats blocked on mobile devices blocked in individual months of 2018.*

Partner's Commentary

Grzegorz Michałek
Arcabit

Year 2018 was not a surprise to us. It presented a coherent and constant continuation of the tendencies we've been observing and researching in our laboratory in 2017. Thanks to the increased user awareness and perfecting protective mechanisms, the number of successful attacks leading to encryption of data and attempt to extort a ransom for their decryption has dropped. Also, our expectations concerning cryptocurrency miners have been met completely – the beginning of the year 2018 brought a tremendous increase in infection attempts with Coin Miner type of software.

The infections themselves were not seen by the users as particularly harmful, mostly because the losses in system performance were not as tangible and often as catastrophic as the loss of data after its encryption. At the same time, detection and neutralisation of the miners proved to be simple enough so that along with the fall in the Bitcoin exchange rate, it resulted in a drop in the number of detections in the following months of the year. We do not anticipate any significant increase in the level of threat with this kind of malware in the incoming months. However, we are still working on tightening up security mechanisms against the most popular vectors of attack. The use of artificial intelligence to e.g. detect social engineering attacks brings excellent results and allows blocking threats at a very early stage of propagation, especially while bearing in mind that the cybercriminals' imagination in the field of e.g. constructing e-mail messages is indeed impressive.

Looking into the future, we expect the cybercriminals will make their move in the field of GDPR and attacks on personal data. Surely, new threats will emerge in this domain, which will consist in forcing victims to pay ransom for refraining from revealing an incident of theft (meaning a leak) of personal data (theft which really took place, or more probably – fictional theft) indicating that the victims have not applied sufficient security procedures to protect the data entrusted and processed by them. Some of the victims will then face a dilemma intensified by both the amount of the financial penalties for not adjusting their organization to GDPR's requirements, and by the fact that still, a significant number of subjects has not taken the steps to fulfil those requirements.

> „
>
> **Thanks to the increased user awareness and perfecting protective mechanisms, the number of successful attacks leading to encryption of data and attempt to extort a ransom for their decryption has dropped.**

4. Current trends in cyber threats

In accordance with the predictions presented in the last year's report, the year 2018 has barely changed in terms of phishing campaign distribution. Polish internet users are still being targeted through the use of social engineering. One could think that after so many years of constant attacks on mailboxes and social media profiles, the awareness of internet users won't allow them to fall for obvious scam. Unfortunately, even though certain improvement can be seen, (this is reflected in the number of the incidents reported) the problem has still not been solved.

Even the "textbook" examples of phishing get to be successful, not to mention the sophisticated ones. This can be seen in the number of issues in our calendar – a large portion of events from the year 2018 consists in campaigns impersonating well-known institutions and organizations.
Year 2019 won't be an exception. Regular internet users, as well as businesses and public administration representatives will be targets all alike.

The experts see large potential for protection against cyber threats in the use of artificial intelligence (AI). These kinds of mechanisms are supposed to support threat detection on the level of user's work station as well of dedicated network solutions or SOC services. Possibilities carried by artificial intelligence can make incident reaction significantly quicker right upon malware detection. Automated identification and threat analysis will be possible thanks to adequate tools employing machine learning technology. This kind of solutions, supported with expert knowledge, prove to be highly successful against series of attacks.

Along with AI, go efforts to make the work of personnel responsible for security as automated as possible. With the current number of threats, manual analysis of all events is no longer possible. The aggregation of massive amounts of data is also a problem, making it difficult to make use of the data in terms of gaining information relevant for security. This is why more and more often SOC and CSIRT teams use threat intelligence solutions, including dedicated platforms. However, to make the most efficient use of such tools, cooperation of analysts is required. It is only when security is treated as a "common good", maximum functionality of products and services can be utilized.

Successful threat detection is an extremely important process. Still, proactive steps, meaning adequate security measures, are of equal importance. A trend which will certainly not cease to develop is the use of authentication based on biometrics. The popularity of such solutions stems from the fact that they're "user friendly". After all, fingerprint, voice, or facial recognition doesn't require remembering complex access passwords. It is also considered to be better, because biometric features are unique – so they cannot be "guessed". Apart from that, this kind of authentication is simply faster. This is why an increasing number of services and devices allow choosing this functionality as a default one.
The flipside? While biometrics is becoming a standard, the question of authentication data security rises. A significant security challenge is then to ensure that this kind of data is being gathered and stored in compliance with good practice, as one can easily imagine the consequences of a leak of biometrics-based authentication data.

4.1 Trends – malicious software

In 2015, we have launched CyberTarcza – a solution for threat detection and securing our customers against harmful software.

We keep on developing this mechanism, especially in terms of detection of various kinds of malware. We employ the most advanced solutions available worldwide, utilize several of the best sources of malware definition as well as our own custom solutions for increasing the efficiency of protection against malware. Our Probes and honeypots are distributed across the entire network.

However, the events of the year 2018 changed our perception of security mechanisms a little, and motivated us to implement further changes within the CyberTarcza. In the report from 2017 we distinguished between threats by the medium of internet access – ones emerging in fixed access networks and ones emerging in mobile networks.
In the year 2018 we have observed that it no longer makes sense to divide network traffic to Fix and Mobile. We keep on connecting our phones to various Wi-Fi networks, so threats connected with Android massively appear in the Fix traffic.
We even hotspot "mobile" internet for PC computers (or gaming consoles even), we use LTE as a basic transmission medium – so PC-specific threats are being detected in Mobile traffic.
The Mobile/Fix distinction ceases to serve any purpose. It seems to make more sense now to categorize malware by "launch" platforms – Android, Windows PC, Linux, and in rare cases - macOS and iOS.

Looking at the year 2018 one can also see some characteristic trends. Apart from "typical" malware such as Triad or Nymaim, incidents connected with offensive ads and cryptocurrency miners have greatly increased in number.

Details concerning typical malware are displayed on the chart below:

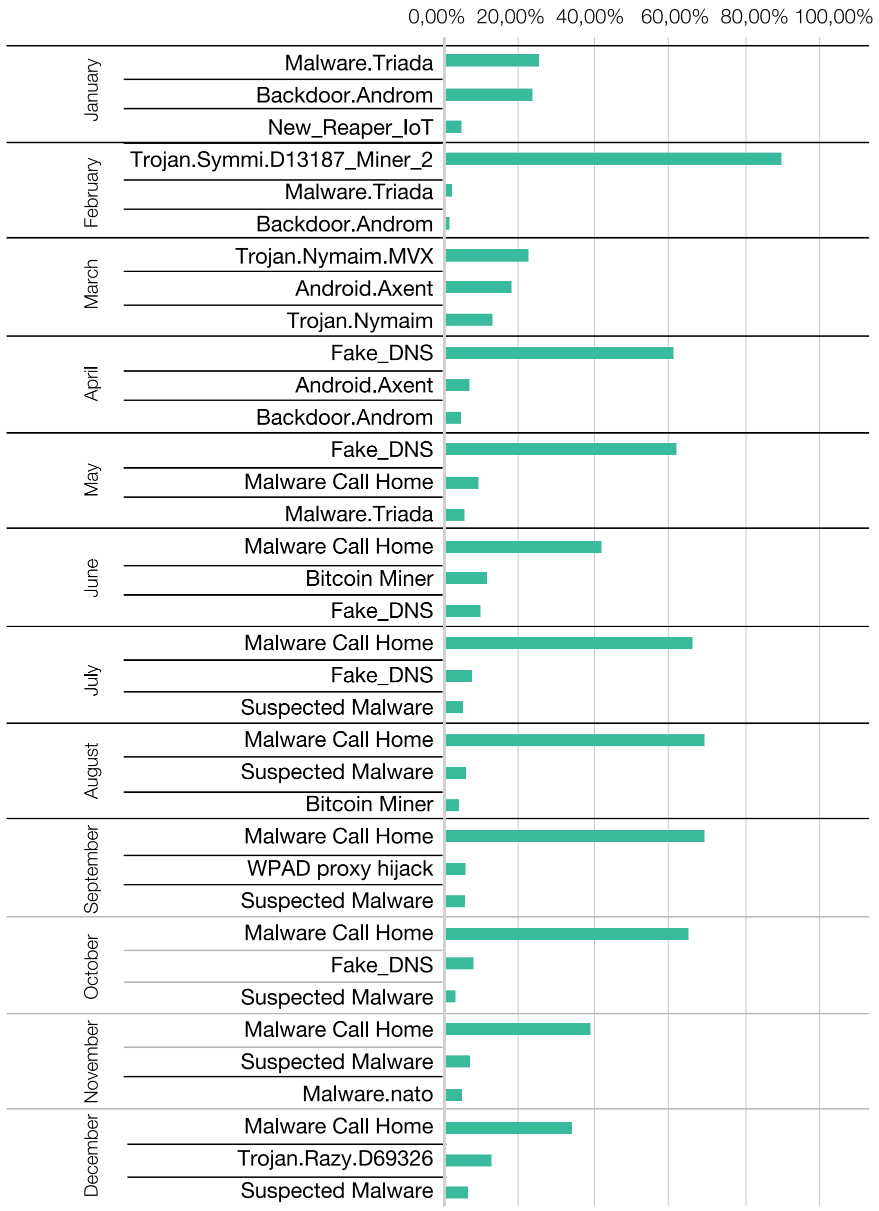


Figure 21 *Details regardin typical malware.*

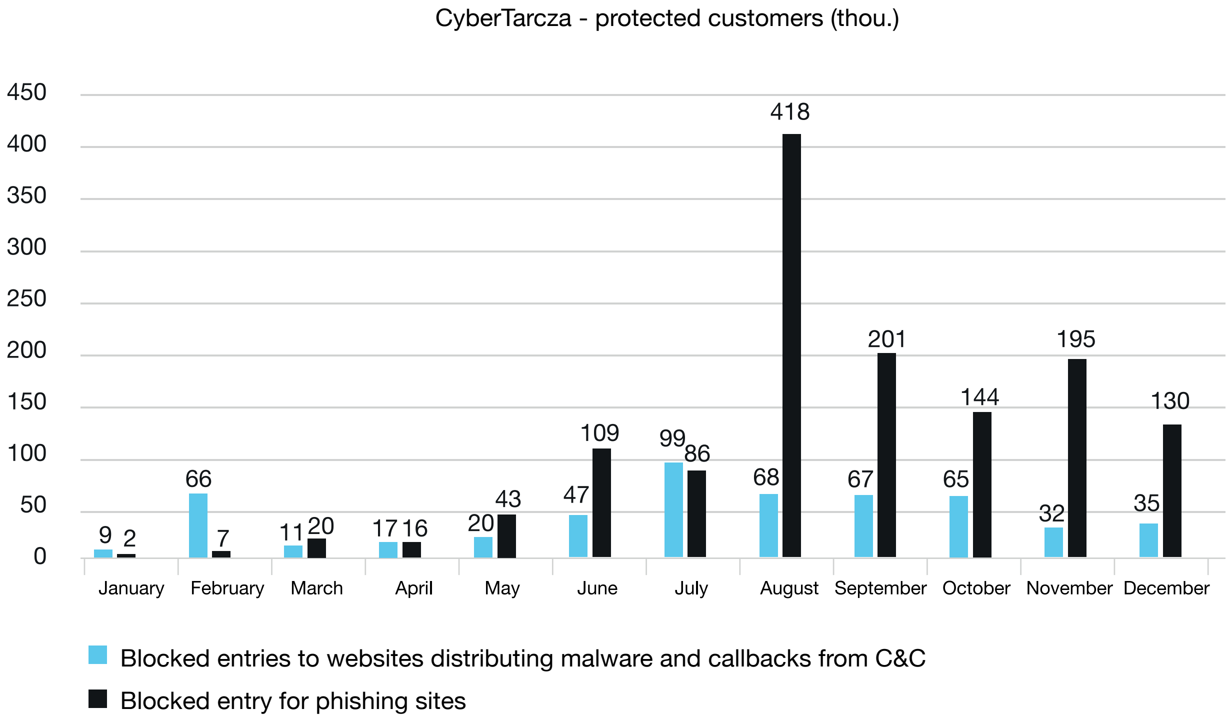


Figure 22 *Unique clients (IP addresses) blocked by CyberTarcza mechanisms.*

In the Orange network we can constantly observe the activity of botnets such as Triad, Andromeda, Nymaim, and Axent, even though these threats have been recognized and are well-known. They are subject to constant modifications, and their activity within networks will probably never be fully eliminated. It is assumed that this may be connected with at least several phenomena:

- network users don't use antivirus software, or the signatures of their AV systems are outdated
- users ignore informational campaigns we convey to them using CyberTarcza mechanisms
- infections are reappearing due to the successful solutions distributing threats in the web, e.g. mailing campaigns distributing newer and newer variants of malware hidden in fake invoices attached to the e-mails.

Since April until the end of July we were dealing with a large scale campaign, in which DNS addresses in the customers' network devices were swapped (e.g. in cases when default logins and passwords were not changed, or upon entering a malicious website doctored to use a vulnerability in modems and routers), or directly in the browser. As a result of the campaign, we have observed 1, 5 million to 2 million of events of queries to "wrong" DNS servers a day. Steps taken by Orange Polska, which concerned almost 19 000 users, along with successful sinkholing of DNS used in this campaign, allowed to minimize the occurrence of this family of threats, but have not eliminated it completely.

The second type of threats, against which we have taken strong action, is the activity of software known as Adware_MB and PUP.Adware. This software usually causes unwanted pop-up ads to display, and depending on the variant, it may also modify default settings of the system and browser (including DNS), encrypt files on computers, extract saved logins and passwords, violate user's privacy, and slow the system down. It may be also used to redirect the user to websites distributing the proper kind of malware. In 2018 we aimed CyberTarcza campaigns towards over 10 000 of users, and this trend will most probably be continued also in the years to come.

We strive to protect the users from a particularly harmful threat called Bankbot_Anubis. It's software meant for Android running devices, usually pretending to be a harmless application. After granting it high privileges (because who reads communicates about application privileges, usually we just automatically allow everything) it reads symbols from the keyboard (logins and passwords), and it targets mostly bank applications. In CyberTarcza, we sinkhole all recognized queries to Command and Control servers connected with this threat.

Another significant action of the CyberTarcza was aimed against Andromeda. We have covered 7000 users with several campaigns within a year, but despite that, the threat still reappears, and is detected in network traffic.

We still observe the activity of botnets such as Sality, Conficker, Necurs, and DanaBot in the network, even though they technically shouldn't exist since many years. Sality has been functioning since around 15 years, while Necurs since over 6 – exceptionally long, bearing in mind current malware trends. There may be several causes of this state of affairs – the criminal infrastructure had been overtaken by the authorities, so the infections are no longer harmful towards users, operators successfully sinkhole C&C addresses associated with these botnets, and malicious use of vulnerabilities no longer takes place. The carelessness of the users also is an important point – such as outdated AV system signatures on computers, or even lack of thereof.

Throughout the whole 2018, CERT Orange Polska Team conducted 89 campaigns in total, which covered over 56 000 CyberTarcza users.

We have also conducted 4 informational campaigns dedicated to password leaks for the users of Orange Polska. These campaigns covered over 13 000 users. The second noticeable trend observed in the year 2018 in the Orange Polska network was the activity of Adware type of software.

What do the statistics look like?

The Figure 23 presents percentage distribution of subsequent categories of Adware in comparison to the total Adware activity in the Orange Polska network.

Even though we haven't observed any significant activity of this type of software in the first quarter of the year 2018, this activity increased with each further month. A large portion of this activity is connected with software identified as one for the Android system. The spread of such threats is multi-vector, starting from Google Play store on devices, through malicious applications purposefully put on the Play store by fake "developers" by bypassing the store's security, ending with traditional means of infection (through messages coercing the user to click onto a malicious link redirecting to an infected website). There has even been a threat which by making use of the Captcha mechanism, could find the device from which the user entered the website. In case of a device running on Android system it would download a malicious file from the BankBot_Anubis family (in this case a thieving text message), and in case of a Windows PC, it would download a .zip file containing JavaScript infecting the computer with the Nymaim malware.

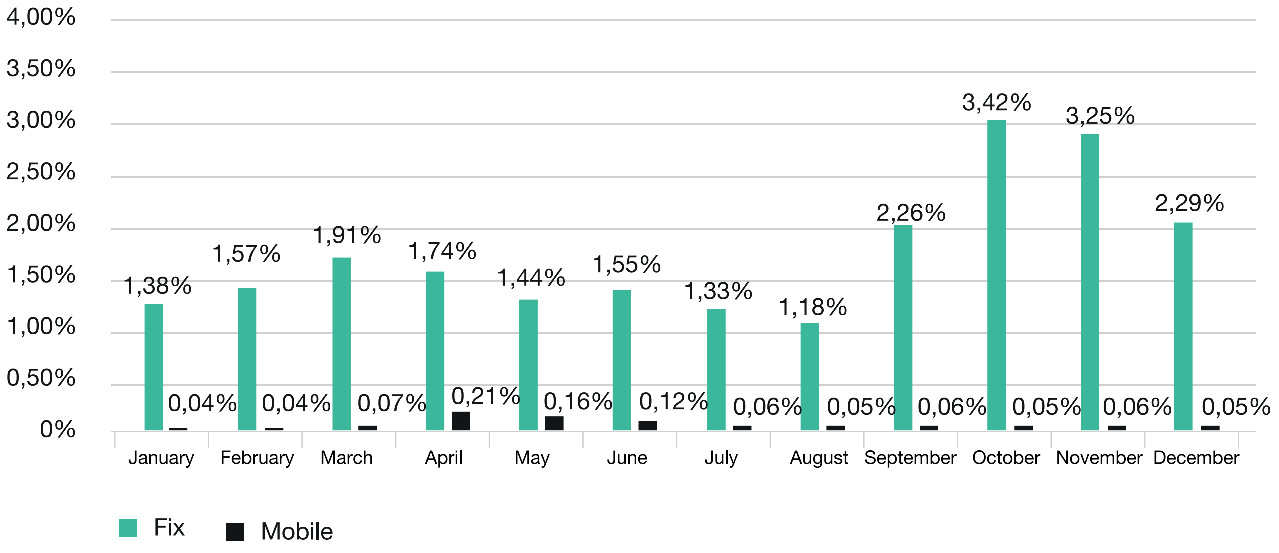


Figure 23 *% of infected customers' networks, in which malware signatures have been detected*

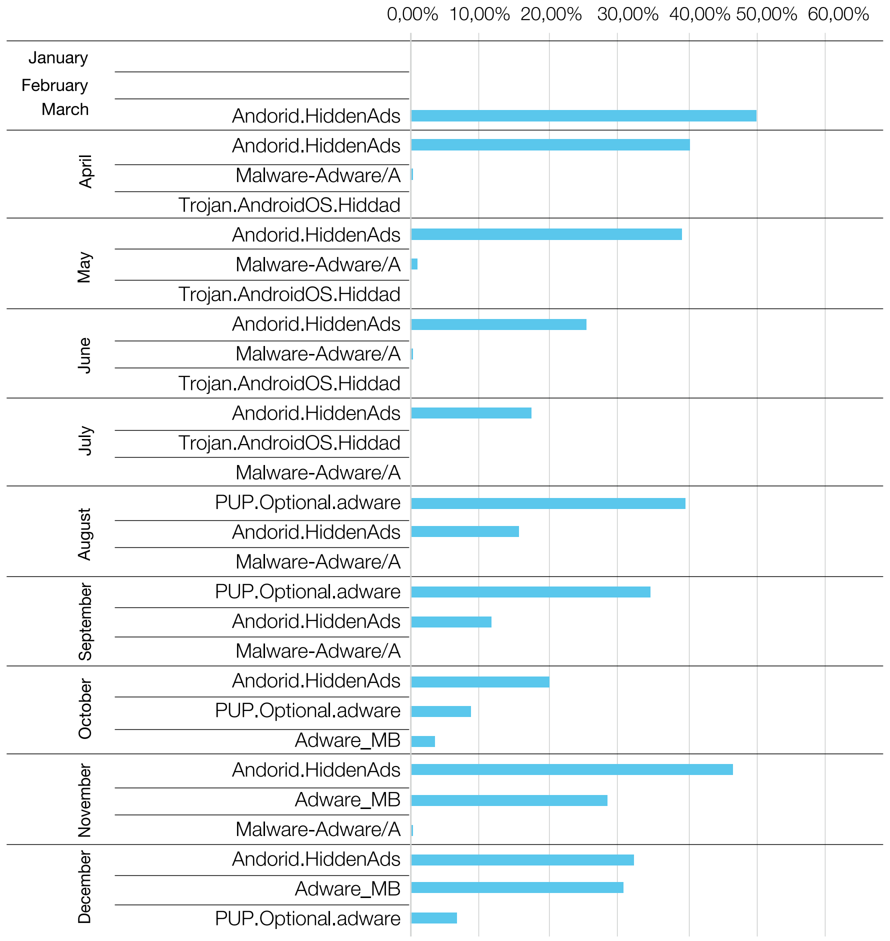


Figure 24 *% of infected customers' networks, in which malware signatures have been detected.*

The campaigns against Adware_MB and PUP.Adware are only a fraction of actions that we take to protect our users from the activity of this kind of malware. Our main way of doing this is blocking communication with Command and Control servers on network level. In 2019 we're going to strive to give Android system users efficient tools for removing malicious software from their devices.

The third trend connected with threats from the World Wide Web, are cryptocurrency miners. The Figure 25 displays miners most popular in specific months in relation to the entire network traffic connected with malicious software in the Orange Polska network. Despite the drop in the value of cryptocurrencies, the miners remain active. This may be due to the fact that the users of these miners do not bear the costs of obtaining the cryptocurrencies. These costs are offloaded onto internet users, because it the computing power of their machines that is used for cybercriminals' financial gain. Not every Orange Polska network user is fond of such use of his resources.

Miner distribution is usually accomplished through scripts placed on infected websites, and less often, through installation of software directly on the users' computers. It is worth t mention, that the activity of miners on websites is not always connected with cybercrime. Sometimes it occurs that website owners place the appropriate scripts themselves. It's a shame though, that they fail to inform their visitors about it. As a curiosity, we may take a look at the research of Technical University of Braunschweig: https://arxiv.org/pdf/1808.09474.pdf. The most popular cryptocurrencies to be mined are Bitcoin and Monero. Even though, the peak of popularity of cryptocurrencies, at least for now, is behind us, the idea of combing "free" computing power of multiple machines and profiting from it seems attractive enough to make the activity of miners to be still visible in the web.

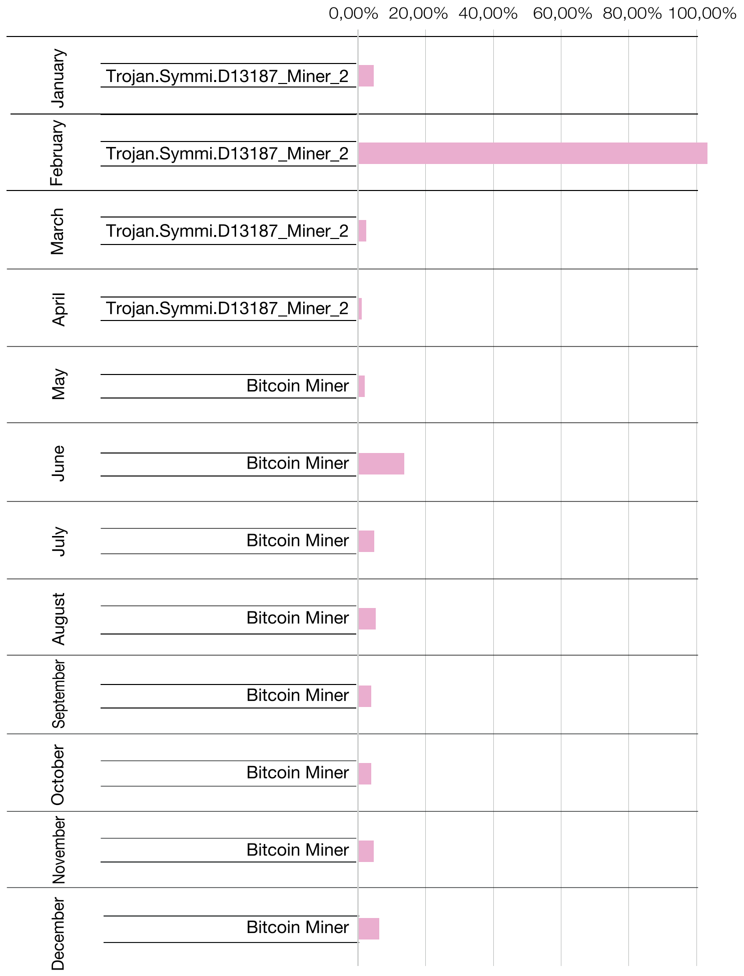


Figure 25 *The most common miners observed in each month in relation with the whole malicous traffic in Orange Polska network.*

4.2 Observed trends of DDoS attacks

As predicted, the frequency of DDoS attacks doesn't decrease. In the year 2018 there was way more of them registered as compared with 2017, although over last few years their frequency remains at a similar level.

Things are similar in terms of the force of attacks, which is also constantly increasing. The average volume during peak intensity of a DDoS attack observed in Orange Polska network reaches 2,1 Gbps, significantly more than in the year 2017 (1,2 Gbps). On the other hand, the highest observed value of traffic intensity during the peak of an attack reached around 198 Gbps (82 Gbps in 2017). The increase in the force of attacks wasn't caused only by faster internet connections, but also attractive prices of DDoS attacks on the black market, as well as the use of reflective amplification and botnets based on Internet of Things devices. It may be also worth to take notice of the trend indicating that the duration time of attacks becomes shorter. **The average time of all the alerts in the year 2018 equalled around 11 minutes (15 minutes 2017). Similar to 2017, most of the registered alerts lasted less than 10 minutes (almost 88% in 2018, a little over 72% in 2017) – an increase of 15% in 2018.** This phenomenon may be in close correlation with the high number of attack on individual users in connection with their high activity in the network, e.g. online games (attacks directed at online gamers – logging the player out) and with easier access to DDoS services on the black market – the shorter attack, the more it is available (smaller cost of service).

In terms of types and characteristics of DDoS attacks, just as in the previous years, the most commonly occurring types of volumetric attacks were UDP Fragmentation (in over 63% of all attacks in the year 2018) and Reflected DDoS (reflective amplification) using UDP protocols (i.a. CLDAP, DNS, NTP, SSDP, CHARGEN) – identified in a little over 80% of all attacks in the year 2018. However, in 2018, the scale of using open LDAP servers has increased significantly.

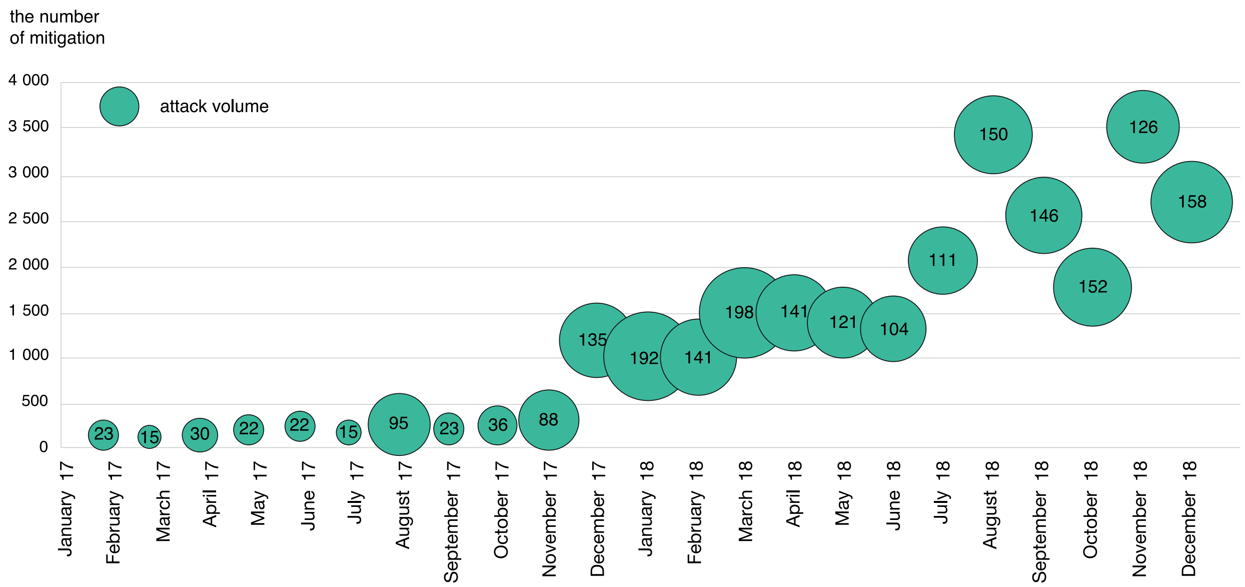


Figure 26 *The number of mitigations (neutralization) of DDoS attacks.*

CLDAP Amplification attacks occurred in a little over 30% of all attacks (The biggest increase as compared to the year 2017, by almost 28 pp.). This type of attack was dominant in almost all large-scale attacks.

As show the first weeks of the year 2019 we can expect the main trends to continue, i.a frequent occurrence of DDoS attacks, with no decrease in their force.

”

The average volume during peak intensity of a DDoS attack observed in Orange Polska network reaches

2,1 Gbps.

the highest observed value of traffic intensity during the peak of an attack reached around

198 Gbps.

Partner’s Commentary

Michał Sajdak,
Consultant in Securitum. He has ten years of experience in issues related to technical IT security. He conducts security tests and audits. Also, performs workshops on cybersecurity. Holder of the certificates: CISSP, CEH, CTT +. Founder of “Sekurak.pl” website.

Better to combat security violations, or sleep easy in blissful ignorance?

Has cybersecurity improved in the year 2018? Are there any new trends? These seem to be the two questions I get asked most often lately. It’s very hard to come up with a clear and satisfactory answer. Let us take a look at some examples, though.

Leaks of passwords and other sensitive user data are a continuously hot topic. Last year, one of the biggest incidents of this type was observed in the booking system of the Marriott hotel chain (several hundred million records of user data has leaked, including several million unencrypted passport numbers): http://news.marriott.com/2019/01/marriott-provides-update-on-starwood-database-security-incident/

Some point to the fact that the unauthorized access lasted (undetected) for several years: https://www.telegraph.co.uk/technology/2018/11/30/private-data-500-million-marriott-guests-exposed-massive-breach/

In the entire 2018, a record amount of information on security violations has been made public. It is among others, because of the regulation coming into force RODO / GDPR) that companies are obligated to disclose these kinds of incidents (ones connected with personal data processing).

To sum up: from my point of view, I can see the following trend: we have more and more mechanisms detecting security violations (which is good), thanks to which more and more companies finds out about successful attacks on their infrastructure (again, good). Then, thanks to regulations, some incidents also become known to regular people (great).

So I’m going to ask a bit ironically – maybe it is better to know nothing, detect nothing, and report nothing? In short – sleep easy…?

What awaits us in 2019?

On one hand, global ransomware campaigns went down a little, on the other – offenders organize more and more elaborate operations, connected with selection of particular victims, becoming more familiar with them, and the final invasion deep into the infrastructure. What is worse, these kinds of activities sometimes bring shocking effects (see: https://sekurak.pl/idzie-nowe-w-ransomware-10-000-000-pln-zysku-w-kilka-miesiecy-dzieki-takiej-oto-wyrafinowanej-strategii/).

It is also worth adding that a successful attack doesn’t always immediately lead to demanding ransom. Such demands may be made after e.g. a year after gaining access to the system. Let us remember then, that even though an intrusion isn’t visible, that does not mean it hasn’t occurred. In 2019 it is almost certain that several spectacular incidents will come to light, which in reality took place way earlier.

I also think that it is only a matter of time for a severe and highly successful attack to emerge in the mobile world (smartphones and tablets). There is no shortage of vulnerabilities there, even in the most basic of mechanisms such as, e.g. image file handling in Android. Is taking over a phone after the user clicks a “normal” .png image science fiction? In the times of common lack of updates in the mobile world – slowly it is becoming a reality (https://sekurak.pl/android-mozna-przejac-telefon-przez-ogladniecie-zwyklego-pliku-png-latajcie/)

5. Control, protect, educate, raise awareness? Or should we?

Pornography, paedophilia, drugs, alcohol, crime, and finally malicious software. An almost complete spectrum of threats awaiting our children in the web, isn't it? The thing is, when we take a look at the statistics of the "Protect Children in the Web" application, things will turn out to be quite different.

Protect Children in the Web is a parental control mobile application offered by Orange Polska. It allows i.a. the control of the applications installed on the child's phone, the time spent using the device, as well as filtering the content available at websites. It is possible to only block certain predefined categories, but also to add websites which regardless of those settings can be available or unavailable to our child. The statistics of our application show, however, that the matter of potential threats looks entirely different than the somewhat ironic suggestion from the beginning.

5.1 Only 5% of websites blocked

Before everything else – and this is a definitely good news – only as little as 5, 38% of attempts to enter websites were blocked by the application. Moreover, this doesn't mean that all those websites were objectively dangerous. This is because Protect Children in the Web allows creating the so-called blacklist, which means adding websites to be blocked from outside of the categories described as dangerous. As a result, among the websites blocked were i.a. addresses classified as hobby (0,02% of the websites blocked), travel (0,85%), religion (0,35%), auctions (3,76%), and health/medicine (0,39%). The largest group, almost 50% consisted in the ones which upon entering were not assigned to any category by the system. Thanks to the default blockade of unassigned websites, the application has not allowed to enter any inappropriate websites appearing daily in the web, but not yet assigned to any category. Speaking of pornography – or in fact sex, alcohol, drugs, violence and hazard, because the Protect Children in the Web application gathers all these topics under one category of "dangerous websites". Entry attempts to this kind of websites consisted in 4, 73% of the blocked attempts, and as little as 0,254% of all websites visited by young internet users. More often (5, 12%/0, 275%) parents would decide to block their children's access to social media services.

Where lays the danger then? - In my opinion, if we were to rely purely upon the statistics presented here, without touching upon the matter of the still relatively low "network awareness" among the parents – we should seek it in the websites that were not blocked – says Michał Rosiak, IT Security Expert.

For years, we have been talking about the slow death of linear television. That is not without reason – new generations long not just for visual content, but also for the possibility of choice. "Our" television cannot provide that, while the Internet, and especially Youtube, can. 3,56 % of the visited websites, meaning 2/3 of what's been blocked, are visits to the most popular video streaming service, or Google searches of such content - visits, which are not inherently blocked by the parents, because "it's just Youtube". In the past year's report we have already noted that technology can be only help, while they key is to work and talk with the child.

Pathological content is but a fraction of what can be seen on Youtube, which is brimming with valuable content. Still, the statistics analysed point out that the Protect Children in the Web application filters a lot of queries, or certain videos connected with exactly self-appointed sex coaches and the so-called patostreamers (eng. pathological streamers). The latter ones are a new, highly disturbing phenomenon – vulgar, humiliating, and violent materials being streamed live online. These transmissions are gaining tremendous popularity, and becoming a very dangerous, demoralising force, as well as the source of income for people responsible for them. More and more often, however, they draw the attention of the police and prosecutor's offices, which ends in fines and bans on online streaming.

5.2 What is actually dangerous in the web?

The analysis of the websites visited by the users of the Protect Children in the Web application provides an opportunity to reflect on what, as parents, should we be wary of. The basis for the parental control applications was most of all, the desire to protect children from pornographic, brutal, and disgusting content. And indeed, they manage to do that, but the repeating addresses of the blocked sites prove that the youth oftentimes know what they're searching for... Still, these threats are only a small part of network activity.

- Throughout the past few years we have regularly provided information about the threat statistics concerning children in the internet. We have described technological solutions, applications, etc. maybe we should look at it from an entirely different perspective? The results mentioned above prove that technological solutions surely are viable. It is equally important to take care of education in terms of cybersecurity in schools, though. I had the opportunity to talk with education workers about the inadequacy of the curriculum as measured against our current times repeatedly. The skill of using an office suite is certainly useful, but my experience with my sons shows that even at the level of first class of primary school a child can understand the importance and process of creating strong passwords, and in further steps, the idea of two-factor identification, or later – social engineering. It doesn't necessarily have to be discussed at IT lessons, since these are topics which will just as well fit into social studies class or conversations at advisory class. We can be easily outmanoeuvred, and the knowledge of that is just as useful as strong protection against dangerous online content – says Michał Rosiak. See also: the "Psychology and Phishing" article.

6. Cybersecurity services in the Act on the National Cybersecurity System

It was already by the end of the last century, that the regulative bodies of the European Union were beginning to receive more and more reports indicating that to effectively counter "cyberviolations" it was necessary for the EU countries to work closely together.

In the year 2004, ENISA (European Union Agency for Network and Information Security) was established, which was to fulfil a role of the centre of competence in the field of cybersecurity in Europe. Still, it was not before 6th of July 2016 that we got a comprehensive legal act concerning regulating the matter of cybersecurity in the countries of European Union. It was then that the Directive of the Eurpoean Parliament and the (EU) Council 2016/1148 concerning measures of a high common security of network and information systems across the Union, known as the "NIS Directive" (The Directive on security of network and information systems).

In the recita 2 of the Directive, we can read that "The magnitude, frequency and impact of security incidents are increasing, and represent a major threat to the functioning of network and information systems. Those systems may also become a target for deliberate harmful actions intended to damage or interrupt the operation of the systems. Such incidents can impede the pursuit of economic activities, generate substantial financial losses, undermine user confidence and cause major damage to the economy of the Union." To ensure efficient mechanisms of combating cyber-threats, the NIS Directive imposed an obligation on the UE member countries to implement adequate regulations in their domestic legal order, which would establish structures responsible for cybersecurity and incident management nationwide, the so-called CSIRTs, meaning Computer Security Incident Response Teams.

In Polska, the obligation of implementing the NIS Directive was fulfilled by the act from 5th of July 2018, on the National Cybersecurity System (Dz. U. z 2018 r. poz. 1560), which along with the accompanying executive regulations, should ensure undisturbed supply of essential and digital services in the country. This act, called also the "Cyberact" in the media, came into force on 27th of August 2018, and established the national system of cybersecurity in Polska, which includes i.a. institutions of governmental administration and the biggest entrepreneurs from the core sectors of the national economy, on whom the act places certain obligations concerning data protection, risk management and incident reporting. Among the entrepreneurs special obligations will fall upon the essential service providers, meaning services of key importance for sustaining the critical social-economic activity, which could be significantly disturbed by IT security incidents. A subject is considered an essential service operator when it meets the following requirements:

– It is listed in the appendix 1 of the act,
– Provides an essential service contained on the list of essential services,
– Providing this service is dependent upon IT systems
– An incident could have significant consequences hindering the ability to provide the service by this subject.

It is then when a competent authority can issue an administrative decision to acknowledge the subject as an essential service operator. The list of the essential service operators is managed by The Ministry of Digitalization, and it is estimated that even 800 of national enterprises representing various economic sectors may make their way to this list, including the energy, transport, banking, financial, healthcare, digital infrastructure, distribution of water sectors, etc.) In as little as three months since the day of receiving the decision of being acknowledged as an essential service provider, the chosen subject will have to i.a. create internal structures responsible for cybersecurity, or call upon services of other subjects that already possess competence and experience in the field of cybersecurity. In terms of the range of obligations imposed on the essential service provider, the obligations which – if the operator decides to outsource them – may be fulfilled by an external subject, the act defined specific requirements which have to be met by the operator's internal structures or the cybersecurity service provider. These requirements are:

1. Meeting the organizational and technical conditions allowing to provide cybersecurity to the essential service operator;
2. Possessing space adjusted to providing services from the incident management field, secured against physical and environmental hazards;
3. Applying security measures in order to ensure confidentiality, integrity, availability, and authenticity of the processed information, with personal, system exploitation and system architecture security in mind.

The detailed process of fulfilling these obligations was described in the Minister's of Digitalization regulation from 10th of September 2018 on the matter of organizational and technical requirements for subjects providing cybersecurity services and internal structures possessed by essential service providers responsible for cybersecurity, according to which every essential service operator has to i.a. ensure that he has circadian support throughout the entire year, with a reaction time adequate to the nature of the essential service. The internal structure possessed, or the provider of external cybersecurity structure has to employ personnel trained and experienced in:

1. threat identification in the context of IT systems,
2. malicious software analysis, and determining its influence on the essential service operator's IT system,
3. Securing trace evidence for the purpose of investigations led by law enforcement organizations.

Apart from fulfilling organizational requirements briefly described above, the internal infrastructure, or the external service provider also has to fulfil technical requirements, i.a. possess:

1. computer equipment and specialized IT tools which allow:

– automated registration of incident reports,
– code analysis of the software deemed as malicious,
– evaluation of the IT systems in terms of breaking security,
– securing trace evidence for the purpose of investigations led by law enforcement organizations;

2. means of communication allowing information exchange with the subjects receiving their service, as well as with the appropriate Computer Security Incident Response Team (CSIRT), working on a domestic level.

As we mentioned, the tasks connected with establishing internal structures, or conclusion of a contract with a subject providing services in the field of cybersecurity should be realized by the essential service operator within three months since receiving the decision to acknowledge the subject as an essential service operator. Within the same period, the operator has to implement risk assessment for his essential services and management of this risk, manage incidents, appoint a contact person with the appropriate CSIRT and a Point of Single Contact with the Ministry of Digitalization, educate the users, report significant incidents to the adequate CSIRT and remove vulnerabilities. In six months since receiving the decision to acknowledge the subject as an essential service operator, the operator is required to implement technical and organizational measures adequate to the level of risk, gather information about threats, apply solutions preventing and containing the influence of the incidents on the security of the IT system, as well as to develop, keep and oversee, in accordance with the act, the record concerning cybersecurity of the IT system used for providing the essential service.

Every essential service operator has to i.a. ensure that he has circadian support throughout the entire year, with a reaction time adequate to the nature of the essential service.

At the moment, many proceedings concerning acknowledging subjects as essential service operators are taking place, and once they're finished, the operators will have to fulfil the obligations imposed on them within a specified amount of time since receiving the decision from the competent authority. It may be worth not to wait with implementation of cybersecurity services complying with the act until the last moment. It should be also remembered that the statutory requirements already apply to digital service providers (pl. DUC) and their fulfilment may be inspected by the competent authority in the field of cybersecurity.

Partner’s Commentary

Piotr Konieczny
The head of the niebezpiecznik.pl security team, a company specializing in breaking into other companies’ servers with their permission, in order to locate security gaps in their IT infrastructure, before the real cybercriminals get the chance to do so.

For most of us, year 2018 was marked by the issue of “personal data”. All this due to GDPR coming into force. Has this regulation really increased our security? The signals are mixed. On one hand, it was this (and only this) regulation that pushed some businesses into attending the matter of IT security in its broadest sense. On the other, how many failures occurred around 25th of May – almost all of them connected with the not always necessary informing (pron. spamming) clients about “increased protection” they can now count on. While boasting about “having conformed to GDPR”, many companies haven’t concealed their clients’ e-mail addresses, and by that actually generated incidents which they should report to President of the Personal Data Protection Office. An incredibly interesting thing about the incidents themselves was the summary of reports from the first month of the regulation being in force. The number 1 cause of most data leaks were… typos, meaning nothing else than the lack of BCC, or directing the content to the wrong recipient. So, not the evil hackers at all...

Unfortunately though, there was no shortage of hacker attacks. The undoubtedly most interesting one was aimed at the Morele web store, which had been detected only through further attacks aimed at the store’s customers. Having gained access to the database, the hacker would send them text messages saying: “additional payment of 1 PLN required. Pay now: link”. Under the link, there was a fake DotPay payment intermediary panel, and if someone didn’t notice that after choosing their bank, he ended up on the wrong domain (which is harder to see on a small smartphone screen), then, after entering password and careless confirmation of the transaction, or inattentive reading of a text message sent by the bank, he would lose all their savings.

The additional payment trick and fake payment intermediary panels was, in fact the most popular vector of attack in the year 2018. It came in all shapes and colours - additional payment for the courier here, or for an invoice over there. These attacks made some people realize that they weren’t capable of safely paying online, despite the social engineering used was not top-of-the-line.

Apart from hackers, Polish internet users were robbed by regular scammers. Regular, yet cunning, and what is worst - learning from their mistakes. First, they would mass send e-mails in which they claimed to have recorded the victim in an explicit situation during his or her visit on a pornographic website. The recording would be deleted after the victim would pay ransom in cryptocurrency. It seems that a lot of people visit porn sites, because the cryptocurrency flooded the blackmailers’ addresses in no time. Many people got really scared. The second iteration of this attack took an even greater toll, this time frightening even those who don’t browse XXX websites on the internet. The offenders would include the victim’s correct password in an e-mail – for added credibility. The victim would believe the blackmailer, even though he has not obtained the password by infecting his computer with a Trojan, but by drawing it from among hundreds of publicly available databases which at some point leaked from various websites (on which the victim surely had an account). Further variants of this attack only got better – content written in Polish, and sender address set as the victim’s address (which was supposed to indicate that the hacker took over the victim’s mailbox).

Unfortunately, the examples mentioned above don’t prove that only careless internet users may become victims. Still the largest sums of stolen money are claimed by groups specializing in making SIM card duplicates with the use of “collectible” ID’s. With the possession of the victim’s number, they intercept authorization SMS from banks – and without any interaction with the victim they’re able to rob his account. Most commonly, the victims are businessmen, and some of them lose millions .

The events of 2018 show that nowadays, each of us exists in the internet, and cybercriminals can find a way to fool each and every one of. It’s a good idea to broaden our knowledge in the field of cybersecurity, understood as e.g. safe use of online banking, or proper e-mail and Facebook configuration. These seemingly minor actions can be significant in protecting our data and money from leaks, because when an offender comes upon us, add sees how much effort he would have to put into robbing us, he’ll throw in the towel and move onto the next victim, the less protected one. There are many sheep waiting for slaughter...

7. CERT Orange Polska Experts' Articles

7.1 Ransomware - the history of the fall, or silence before the storm?

Alongside those giants striking mainly at enterprises, ransomware varieties distributed by Malspam raged. No wonder, then, that most predictions for 2018 foresaw more of the same and better quality. As it turned out, these forecasts turned out to be largely erroneous.

In Poland, the changes started in January, when Nymaim, promoted in Malspam campaigns and regularly delivering file-encrypting modules to the stations, switched to software stealing credentials and passwords to banking and postal websites and other popular web applications.

For the first time since the publication of the CERT Orange Polska report, ransomware activity decreased, by only 4%, and in relation to all events detected in 2018, almost by

20%

compared to the previous year.

This trend continued for the following months, and the number of cases of ransomware infection, although still visible, decreased significantly. For the first time since the publication of the CERT Orange Polska report, ransomware activity decreased, by only 4%, and in relation to all events detected in 2018, almost by 20% compared to the previous year.

The so-called "fall" of the ransomware consists of several factors. Last year's success of large campaigns is the first one. Ransomware became famous not only in the world of IT security. Public media raised this topic in the news, special programs were created, and websites regularly posted news about current campaigns and sets of advice on how to protect against infection and how to deal with it if it happened.

Other reasons include the rapid increase in cryptojacking, used instead of ransom requests to generate potential profits in virtual wallets of criminals, reduction in the proportion of income in relation to the costs of running a campaign or mere weariness of materials.

The growing number of clients of cloud solutions, both those offered for companies and services targeted at private individuals is also meaningful. In such a scenario, the threat of encrypting several files on the disc, while most of the critical data is stored relatively securily in the service provider's infrastructure, simply fades. The more so when criminals want a decent amount of money for decryption. The previously mentioned GandCrab demanded the equivalent of $500, that is, the amount for which you could buy a budget laptop, or a few good discs, AV licences and something more.

Putting the matter this way, it may turn out that the path from a successful attack to obtaining any funds from the ransom demand does not have to be easy. Not only do they have to find their way to the user who has no other sources of backup, the victim must get access to the cryptocurrency, in which the ransom is accepted, the procedure of means transfer itself may fail due to imprecise instruction or an error on the part of the user. No wonder that in the face of such obstacles, many criminals began to view cryptojacking as a quiet, harder to detect, and much less troublesome alternative.

It is far too soon to discard ransomware from the list of significant threats. Cryptojacking, as well as cryptocurrencies on the stock exchange after a sharp boom, begins to fall to the ground, the question is whether criminals return to the old, already tested methods.

There are many reasons for this. Although well-known brands such as Locky, Cerber and TorrentLocker almost disappeared from the cybersecurity radar in 2018, many smaller followers appeared, and the number of encryption software variants has never been bigger. Compared to last year, one thing has changed - their application.

In addition to the already described GandCrab, whose creators offer their solution to other cybercriminals as a paid service, and a few smaller players (such as GlobeImposter observed in 2Q2018), the business model ceased to consist in infecting as many personal devices of random users as possible, in the hope that at least one person in ten will think about payment.

The hunting season has begun, and the attacks started to become more and more focused on objectives, from which the chance of means extorting is possibly large. A model example is the criminal group responsible for SamSam ransomware, whose software has hit healthcare and state government organizations in the US.

Instead of massive infections, there were targeted campaigns, instead of an immediate infection right after the software was delivered to the disc, there was a gradual surveillance and identification of the most sensitive data and the most critical systems. Often, as in the case of an attack on the city hall in Atlanta, the initial infection was not carried out by spear phishing, but by brute force techniques, which break weak access passwords to employees' devices with an open remote access protocol.

Ransomware has also changed in the code structure. It is using more and more often polymorphic techniques that change the checksum of a file in order to avoid signature detection. These techniques also extend the encryption time or limit the number of simultaneously "supported" files to circumvent the preventive methods operating on behavioral rules.

Of course, attacks targeted at public sectors or healthcare infrastructure are not accidental also for another reason. Such institutions often use obsolete operating systems whose "best-before" date passed several years ago, and the last security updates were made several years ago, if at all.

The magnitude of vulnerabilities, the lack of apt means of detection, and the constant need for retaining continuity of operations is the ideal environment to conduct any attack, and ransomware, having the ability to immobilize critical infrastructure elements, is the number one choice.

The question whether ransomware will cease to be influential, or its numerous creators, while waiting for an attack, are invigilating the infrastructure of unaware enterprises, is therefore still valid.

7.2 Malvertisement – A Full-Blown Business

Malvertisement is a type of a network attack where the code, hidden directly or indirectly in the displayed advertisement, infects the device of the victim with malicious or potentially harmful software.

Modern marketing has long discovered that the golden rule of politics: "Nobody can give you as much as I can promise you" is perfect for creating advertisements. The same rules also apply to malvertisements, which made up a third of all threats identified in the Orange Polska network in 2018.

Colourful banners, eye-catching enticing slogans, promises of rewards, nudity and taboo-breaking content are the most common backdrop to the distribution of such advertisements.

In case of this threat, the trustworthiness of the website being visited is less relevant; an advertising banner can attack from beyond your screen when you are browsing news portals, as well as when you are downloading software from a source that is not necessarily legal.

Naturally, the nearer to the grey area, the greater the opportunities for cybercriminals to publish their own content. First of all, users of websites that offer the viewing of the most recent films and TV series online without paying for the services of Netflix, HBO and Amazon tend to be more determined to wait until all of the advertisements have played, close all pop-ups that appear in the meantime, and sometimes even to disable the browser protection, which can block the display of unwanted pop-ups with varying degrees of success, during the loading of the video.

In the face of a new episode of Game of Thrones, safety of one's own data – from means of payment to private photographs and social media passwords – is pushed to the background.

Considering the above scenario, one could hazard a guess that the prevalence of malvertisement at endpoints is therefore caused primarily by the low awareness of users, who treat such malicious activity as an ordinary intrusive advertisement or something which any anti-virus software will be able to handle without any trouble.

This is largely true. But that is not the full picture. As we have already mentioned, the lion's share of infections, thefts and extortion uses axioms based upon people's associations. People used to online payments do not hesitate to open an invoice sent by an electricity supplier, and those redirected to a false Paypal page, deceived by a request to

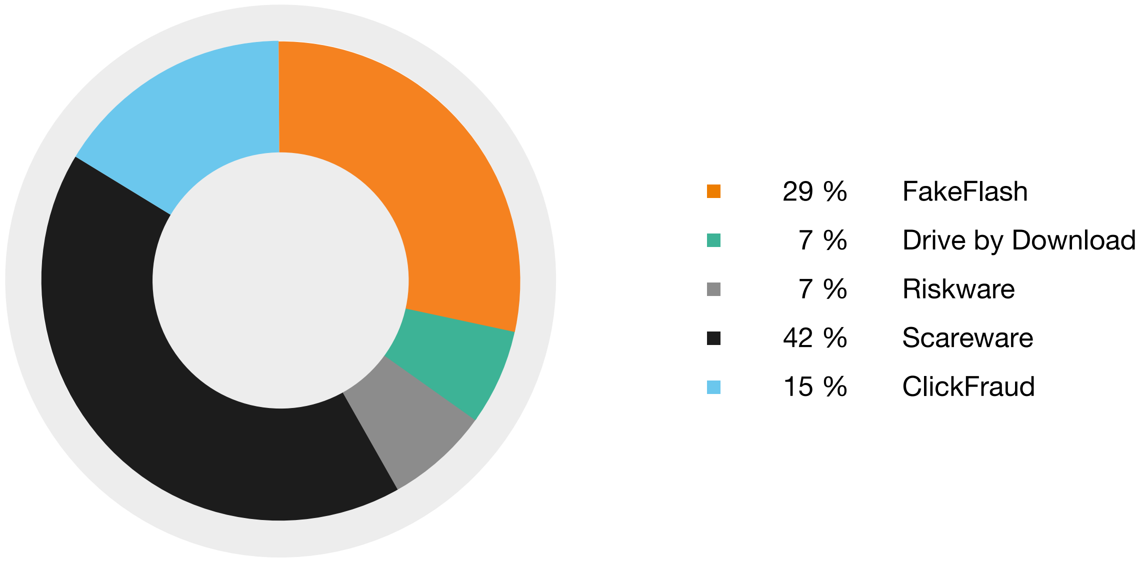


Figure 27 *Types of Malvertisment identified in 2018.*

make an additional payment for their courier delivery, usually do not give much thought to how such a strange discrepancy could arise.

Malvertisement is based upon the same formulas, whilst having a much broader range of options at its disposal.

As indicated in the above graph, only 7% of all advertisements redirected users to websites from which malware was delivered (usually through exploit-kit packs) to user stations.

The overwhelming majority were occurrences where cybercriminals used carefully prepared visual, or sometimes even audiovisual content to attempt to convince a user to interact with a given advertisement on their own and in good faith.

False notifications of the need to update Adobe Flash Player were the leader in this regard; therefore, social engineering has also joined the list of well-known and extensively discussed Flash vulnerabilities.

That campaign delivered to stations a cryptocurrency miner Monero Xmrig, which is also used by some users on purpose and is therefore not regarded as malicious by definition by AV engines.

Everyone knows about FakeAV. This tactic, dating back to the early days of malware and aimed at making a user feel threatened and forcing them to perform a specific interaction, still regularly finds victims willing to pay for the "full version of the software", download an additional application, or call a number provided on the screen, debiting their account with an astronomical sum.

However, numerous successful campaigns demonstrate that scareware does not need to be so scary. More and more often, a successful extortion requires but a false special offer or a phony contest, where you need only to provide your data and pay for the delivery in order to claim the latest iPhone as your prize.

To this date, no antivirus has ever dealt with the problem of human naivety, which is precisely the greatest vulnerability of the terminals of Internet users.

7.3 Threats in the Internet of Things

The so-called smart household appliances are a topic for a separate publication. Much can be said about the reasons and ideas behind the concept of the integration of utility objects within the network which manages them. Much can be said about the business emerging from that, and about its bright and decidedly dark sides. There already are many conspiracy theories, and there will be even more to come in the following years.

However, regardless of the actual reason, the manufacturers of devices comprising the Internet of Things do not lose sleep over the need to protect them. Apart from the issue of exploitable software, users rarely receive any guidelines on the need to change their password following the initial configuration or any notifications when an update for the software operating on their devices is released. This problem is raised to the third power when we are dealing with cheaper Chinese alternatives for devices advertised on the market, whose availability is directly proportional to their vulnerability.

Such glaring loopholes make it irresistible for cybercriminals to ignore the temptation of accepting the invitation. Smart devices are much easier to take over than personal computers and can often play just an important role in the household infrastructure. Due to the low awareness, nobody expects their washing machine to begin mining a currency for a cybercriminal instead of washing laundry, and their inconspicuous fridge to participate in an attack on Poland's largest hosting company.

Household network devices are naturally the most vulnerable to attacks, but the attacks by no means stop at them. Criminals strike at ports listening at Telnet, SSH and RDP protocols, effortlessly breaking the default access passwords. Once they gain control over one of the objects, they spread out, using Version 1 of the still ubiquitous SMB service, adding more pawns to their expanding botnet zombie network.

In addition to those fundamental vulnerabilities, we have also observed in the network some attacks exploiting port 7547, used to disseminate hybrids of last year's Mirai and Hajime family malware, for example, in campaigns against Mikrotika routers operating on RouterOS versions below 6.38.4.

In spite of its usually very meagre computing power, the IoT sector has also been used to mine cryptocurrencies (vulnerabilities CVE-2014-8361 and CVE 2017-17215 on some Huawei routers, and security vulnerabilities in the remote management interface of Claymore – an Ethereum miner – enabling the replacement of the miner's wallet with the wallet of a cybercriminal).

However, the most common threat identified in the Orange network has been VPNFilter, which attacks network devices. This malware has stood out against other threats found in the IoT for various reasons, such as its modular structure. In 2018 alone, it enhanced its code with new functions several times. It has been capable not only of stealing access data processed on the device, but also of injecting malicious code into the websites visited, booting up in Crontab's task schedule, and storing its configuration in the NVRAM in order to hinder the cleaning of the device infected. Moreover, in order to protect its C2 servers from being identified, VPNFilter uses TOR nodes for communication, and can sometimes download some of its instructions in the form of fabricated female model photos containing embedded code and published on a popular photo-hosting website (photobucket.com).

The above example serves only to confirm that IoT threats are increasing not only in number, but also in quality, and aside from their traditional use for DDoS attacks, criminals are using other methods for theft or extortion of resources – from cryptojacking to Man-in-the-Middle attacks – with increasing frequency.

That is why it is so important to take the following several basic precautions during the installation of any device directly or indirectly connected to the Internet:

- restrict or disable access to the devices from non-local networks, and if remote access is necessary – use a VPN client and two-factor authentication for it,
- remember to set or change passwords from the default ones assigned to the devices to new ones, preferably no shorter than 8 alphanumerical characters, including lower- and upper-case letters and special characters,
- close all unused ports, even within the local network. If you do not use the Telnet or SSH protocol when accessing the router, do not leave that door open for an unbidden guest.

It is possible that the number of smart devices installed in houses will soon exceed the total global population. In that case, you need to think about your own security now, before it is too late.

Piotr Kowalczyk

7.4 Malicious code in Orange Polska network (analysis)

Although the number of anti-malware suppliers on the commercial market is constantly growing, and open source solutions are an increasingly reliable source for fresh information about current threats, malware is still doing well, and in some respects it has never been better. Despite more and more complex detection mechanisms, bolder attempts to use artificial intelligence and machine learning techniques, cybercriminals have not fallen behind, and the products they make are gradually evolving, and thus do not allow stagnation to enter into the cybersecurity world.

7.4.1 The biggest threats of 2018

The beginning of 2018 began with an earthquake. An error in the architecture of Intel processors (as well as in AMD of some configurations) has been published. The error resulted in a hole in the security devices of an operating system, which allows Kernel memory to be read from the level of an user. The published patches guaranteed separation of the kernel memory from the user's processes, but as a result processor's work was slowed down by over 60 percent.

The vulnerabilities used were quickly defined for two possible attacks: Meltdown and Spectre, whose capabilities to read data from memory, also contained passwords stored in encrypted password managers, encryption keys and any sensitive data processed on the computer.

In January, as a result of continued attacks of the keylogger campaign on websites and WordPress blogs, 2,000 subsequent websites have been infected. Apart from the script which steals passwords used for authentication, criminals placed a script on the infected websites to dig through cryptocurrencies in the browser by unconscious victim users. It was one of the first signs of the cryptojacking epidemic spread in 2018, which continues to this day.

The following months brought, among other things, an attack on online stores using the large eCommerce service - Magento (in Poland it covers about 5% of all online stores). The attack involved injecting malicious javascript into the source code of the website, whose task was to intercept payment data and data used to log in credentials.

Card Skimmers, i.e. scripts that read data from payment cards, once again were in the spotlight due to the attack on British Airways in September last year, when Magecard (the software was named after the group of cybercriminals who stand behind it), using vulnerability hole in the js - Modernizr library, added 22 lines of a code to it to steal data from over 380 thousand users.

Zero-day vulnerabilities also affected network devices. The most known gap was found in the Router OS system used in the routers of the Latvian company Mikrotik. The vulnerability was connected with buffer overflow in the SMB service during the processing of session request messages, which allowed remote operations to be performed in the system without authentication. Additionally, the Botnet, to which the devices intercepted in this way are attached, has the mechanism to infect subsequent devices available in the network with the same vulnerability, which allows to carry out large DDoS attacks.

7.4.2 Malicious code in the Orange network

Threats were not in short supply in Poland, either. Starting with the recurrent Malspam campaigns pretending to be banks, through network operators, public institutions to courier companies.

A new infection vector proved to be text messages informing about a small underpayment, impersonating courier companies, operators or online stores, which placed in their messages links to carefully crafted online payment services, such as dotpay, extorting this way credentials from victims.

Spoofing has also been used extensively in campaigns conducted for mobile devices. The vector was the previously mentioned fake text messages, but also ads that redirect the user to websites calling for updates of the browser, antivirus system or encouraging to download an application onto mobile devices. In the last case, the software had not only the ability to access text messages (including those with codes for authorization of bank transfers), but also to generate its own notification templates used for Man-in-the-Browser attacks.

The abovementioned techniques of extortion and infection were also joined by sociotechnical messages returning after a break and prepared more or less in Polish, for example the so-called Sextortion scam. Money extortioners used one of the victim's passwords to increase the credibility of the fraud. It could be made public during one of many data leakages, which occurred regularly in Poland and in the world. Last detections contained, in turn, links whose launch resulted in the infection of malware, including ransomware.

However, the largest infection vector remains Malspam, which is presented in the graph below. The graph shows data collected on the basis of research conducted based on the analysis of a sample of monitored FIX and Mobile network traffic.

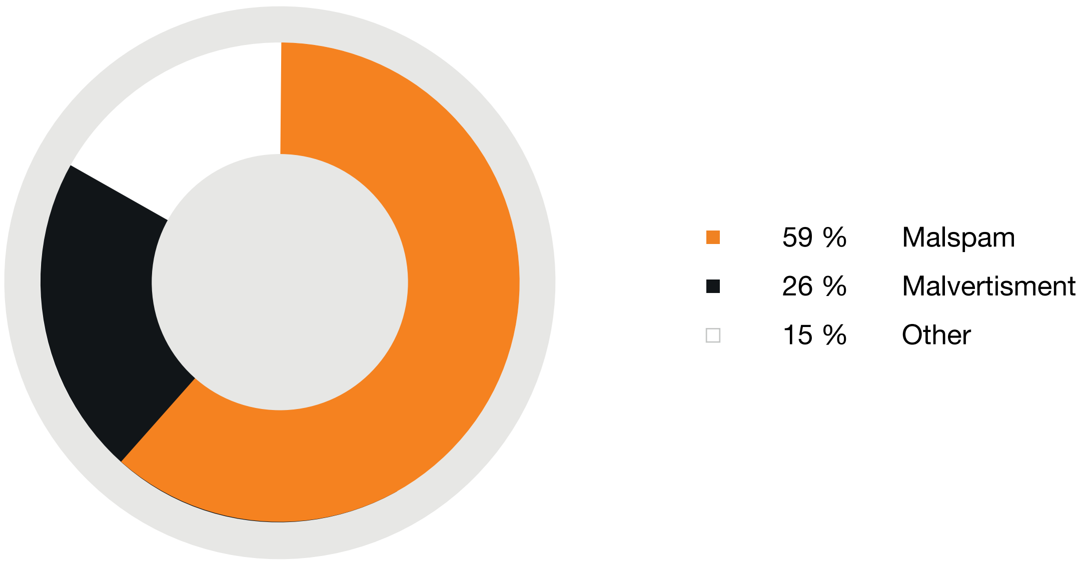


Figure 28 Malicious code vector infections in 2018.

The identified threats directly or indirectly connected with malware activity are divided into three groups by CERT Orange Polska:

- Malware object: delivery of malicious software to the end station, e.g. via an attachment with an executable script
- Web infection: infections with the use of browser vulnerabilities by means of the exploit kits, as well as all malvertisement websites that persuade a user to download and execute a malicious code under the pretext of updating / repairing one's software.
- Malware callback: confirmation of the successful malicious code launch through the combination of network communication with the remote management server (to download further instructions or to transfer the intercepted information).

Similarly to the previous year, among all the detected events, communication attempts between infected stations and C&C servers were dominant (85% of all the events) The figures cannot be surprising, given the varied frequency of single station queries within a given botnet. Compared to the previous year, the number of malware samples downloaded to the final stations increased (over 80%), and the number of detected browser infections increased over ten times.

Malware Callback	Malware Object	Web Infection
2 331 165	128 125	275 088

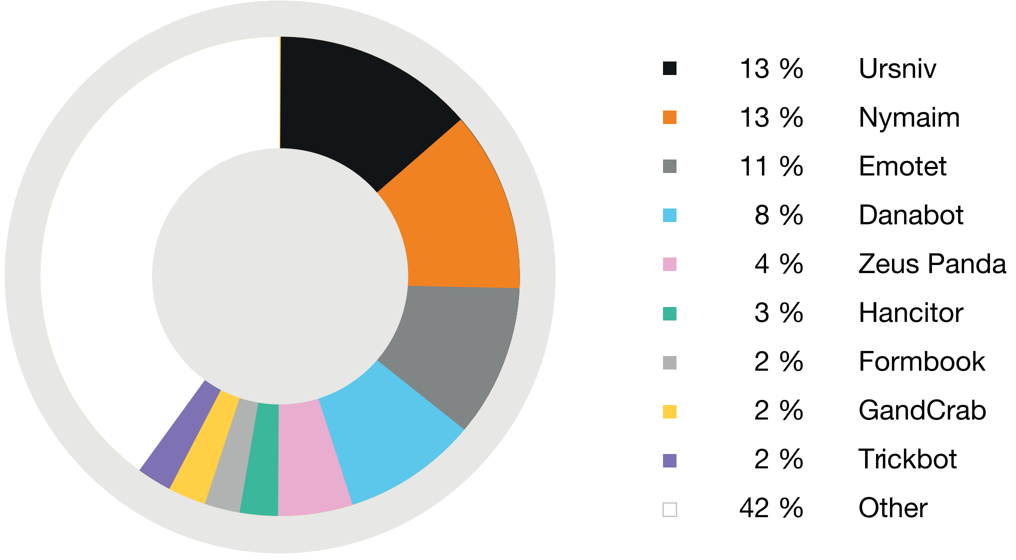


Figure 29 The most common malware families in 2018.

As the Graph 29 indicates, the largest number of users have been affected by campaigns that are already well known to Poles, namely the botnets. Ursnif, Nymaim, Emotet are malware families that have been in the environment for years, and their subsequent versions are a reminiscence of development that has become a part of the cybersecurity and cyber threats sector.

Ursnif, aka **Gozi** is an infostealer, whose part is the "Dark Cloud" Botnet, operating mainly in Asia and Central and Eastern Europe. Thanks to the use of fast flux techniques, allowing IP addresses to rotate for domains exposing malware and servers managing it. Ursnif makes targeting appropriate Command and Control (C&C) servers and their closure more difficult. The infection alone in the victim's system uses "fileless" techniques, i.e. it executes them in the internal operating memory of the system and does not leave their own files on the victim's disc. The files with data stolen from the victim's system are compressed in the CAB format, making the detection of exfiltration more difficult.

Nymaim, Emotet, Trickbot and **Hancitor**
have also undergone changes recently. To infect a system, modules sending spam, infostealers or ransomware are delivered to the modules of different use, such as keyloggers. Trickbot used in encryption with an AES key added a XOR layer. Nymaim has been updated and now has a reinforced code obfuscation with the use of code-flow and stack code techniques to make it possibly invisible and difficult to detect. The evolution of Emotet from the banking Trojan to the modular provider of another malicious software was described a lot in 2018, and from the second quarter last year together with Haciter it is the most systematic malicious software distributed through Malspam campaigns in Poland, providing stations among other things with the most popular banker in the ranking - Zeus Panda.
Zeus Panda.

Formbook is another form grabber in the ranking, whose activity in the first half of the year made it possible to take the place in the top ten. One of its most interesting features is the ability to insert ntdll.dll library from the disc into the memory and to launch the exported functions directly in the memory without the use of API.

Danabot was released as late as at the turn of the second and third quarter last year, and its campaign was mainly aimed at users from Poland and Italy. It spread through numerous Malspam campaigns, and the vbs script that delivered it to the stations was tagged as Brushaloader. Malware alone stole login data to banking services, using to this end a set of crafted web injections injected into the browser the moment a user was visiting the bank's website. These attacks, although they are no longer a new phenomenon, impressed in terms of the number of banking websites for which scripts aimed at stealing data were prepared.

The only ransomware on the list of the most common threats is the **GandCrab**. functioning in the ransomware-as-a-service model. GandCrab's beginnings were not easy. Soon after the initial campaign, it turned out that the web server storing private keys to decrypt victims' files had been attacked, and the data contained on it had leaked to the network. The initial bloops did not discourage its creators from further work, and subsequent releases (in 2018 alone we observed at least five) brought small changes to improve the functioning of the code and to make its detection more difficult. GandCrab was mostly distributed in Poland through the Exploit Kit packages: Rig and Grandsoft. To a lesser extent, it found its way onto victims' computers also through malspam or as malware provided by other downloaders infecting stations. For file encryption, it uses a fast-acting TEA algorithm, and decryption fees are charged in the DASH cryptocurrency. Interestingly, in the sample analyzed by us, the ransomware stops working if it detects that the language of the keyboard is Russian.

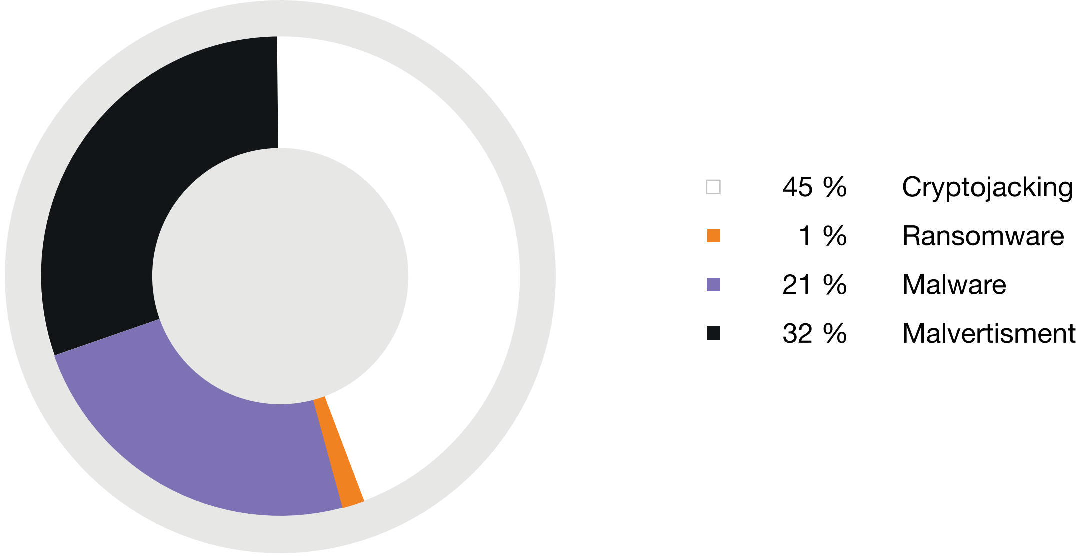


Figure 30 Types of threats detected in 2018.

7.4.3 Malicious software in the mobile network

Malware Callback	Malware Object	Web Infection
787 103	37 286	260 855

While Windows is undoubtedly the number one platform for malicious software, year by year owners of mobile platforms are increasingly exposed to malicious activity threatening their smartphones, tablets and other Android and iOS devices.

After all, mobile devices, thanks to their convenience and widespread availability, are the carrier of the most sensitive information, such as contact lists, text messages or photos. It is the mobile devices which we use to browse social media, carry out banking transactions or do online shopping.

Although both Google and Apple manage in an increasingly restrictive way the applications added to their own stores by active scanning of new items, last year once again confirmed that the malicious content reaches the Google Play store or Apple App Store, too. Especially in the Google store, the presence of spoofed applications is nothing new. Not all of them, however, are carriers of malicious software, but well-crafted social engineering can bring greater benefits than the activity of a malicious code.

Over 97 percent of all events on mobile devices detected in 2018 concerned the Android system. Its greater openness allowed malicious software developers to prepare, test and put into circulation their product much more easily than in the case of the Apple system.

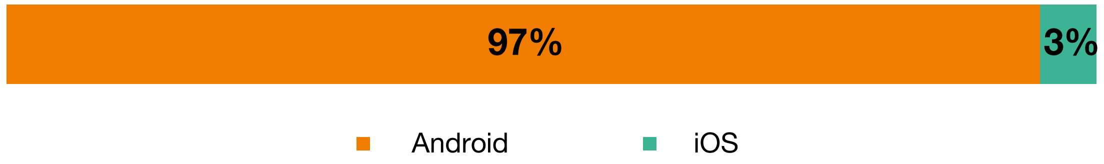


Figure 31 Malware code occurence according to the operating system.

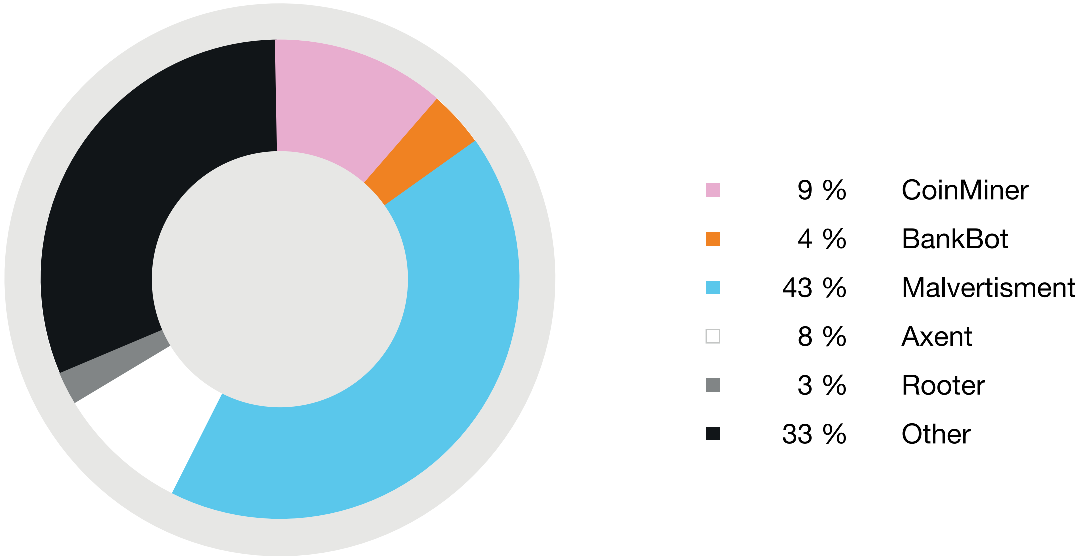


Figure 32 The most common malware in mobile network in 2018.

Malvertisment is one of the most profitable malicious activities in the cybercriminal environment, and mobile devices, along with the Windows platform, are the target of an attack. We have written in an article about different ways in which ads can be used to distribute unwanted or malicious software to end devices. What distinguishes mobile devices from the Windows system is the number of events generated by the Clicker software. Under this concept, we understand software or scripts embedded on websites responsible for events from the click fraud family. Click fraud is a phenomenon of fraudulent clicking on advertisement links settled in the pay-per-click system. Such clicks are aimed at stopping the display of a given advertisement through exhausting the limit for which the advertised company paid or through extorting additional money. According to data obtained from the global Federation of Advertisers, the practices of fraudulent clicks bring over 19 billion dollars annually. For the click fraud phenomenon the following may be responsible: unfair competition, webmasters of websites who make money from displaying advertisements and artificially raise the number of views on the websites they manage or else organized crime groups. It is the latter who are responsible for creating and distributing applications that, when launched in the victim's device, generate false clicks on ads which the user has not actually seen.

Mobile devices also faced the phenomenon of cryptojacking. Despite their lower computing power, applications designed to dig cryptocurrencies flooded the Google Play market, as well as accessed the Apple platform.

Analyzes carried out by the CERT Orange Polska team indicate that the majority of the distribution was made with the use of advertisements, prompting the user to download software to optimize device operation or a free and extremely effective antivirus. Google, as well as some other real AV engines, does not regard cryptocurrency excavators as malicious applications. That is why, in practice the very process of detecting and allowing such software remains uncontrolled.

Of course, cryptocurrency excavators and views' raisers are not the only ones that use impersonation. In 2018, many Polish Android users fell victim to the Trojan **BankBota**. As the name suggests, the purpose of this malware are payment operations. When an infected user opens one of the bank applications, BankBot's code is activated and it creates an overlay for a real bank application (we identified 15 unique overlays to Polish bank institutions). The activated overlay imitates a fake login window by stealing the credentials entered into it. BankBot also has the function of reading text messages, so when the verification code reaches the user's phone, cybercriminals can use it to confirm their own transactions carried out from the unconscious user's account.

Throughout the year, at least a few BankBot's hybrids appeared, and the phishing application was the main actor in phishing campaigns impersonating as BZWBK bank (a fake application in the light version in the official Google Play store), InPost (text messages with a link to download a fake application), as well as some malspam. Interestingly, in malspam criminals provided the function recognising the victim's operating system and in the case of the identification of the Microsoft environment they distributed to download Nymaima instead of an appropriate Android app.

Phishing campaigns' distribution for text messages was common in 2018, and users were flooded with messages from fake couriers, operators and sellers informing about underpayment and giving a link to settle the payment. The link of course redirects you to a crafted website, and it is quite clear what happens after you have entered authentic credentials.

> **Analyzes carried out by the CERT Orange Polska team indicate that the majority of the distribution was made with the use of advertisements, prompting the user to download software to optimize device operation or a free and extremely effective antivirus.**

Cybercriminals understood that this channel of distribution is even more vulnerable than e-mail servers protected by anti-spam and antivirus applications, and anyone can send spoofed text messages about any topic. That is why, it is so important to verify the domain of the website you visit every time you log into bank websites (and into all websites requiring credentials). Any solicitation for payment sent by e-mail or text messages should be verified at source, preferably with the use of a different channel of information (e.g. phone)

7.4.4 What is waiting for us in 2019?

Ransomware, although it experienced a small decrease, is still a real threat. The browser cryptocurrency excavators did a great job in their full-year debut as a substitute for advertisement, and spear phishing continued to terrorize the victims' devices effectively, extending operation methods with text messages and social engineering.

2019 will not bring improvement in this regard. Wiper-type destructive threats, that were very successful in 2017 and experienced a much calmer time in 2018, may come back. Similarly like ransomware, which in the face of diminishing fashion for cryptocurrency excavators on end devices, has an opportunity to successfully return to the status of top threats. Also the development of infections with the use of "fileless" techniques, which will make signature detection almost completely archaic, is worth attention. What is also worrying is an increasing number of methods to use the IOT sector in cybercriminal activities, and botnets made up of hundreds of thousands of infected devices may grow instead of diminish in the near future.

Let's add to this the range strength of malvertising campaigns that provide malware, uncertainty of security solutions in the cloud and the constantly refined methods of obfuscation or shorthand? All of this presents not very bright, though undoubtedly interesting vision of this year.

All of these predictions, however, may be wrong and only time will tell what cybercriminals will give us in the upcoming months. After all, their ability to instantly adapt to new, discovered vulnerabilities or developed tools is the biggest threat in cyberspace.

Piotr Kowalczyk

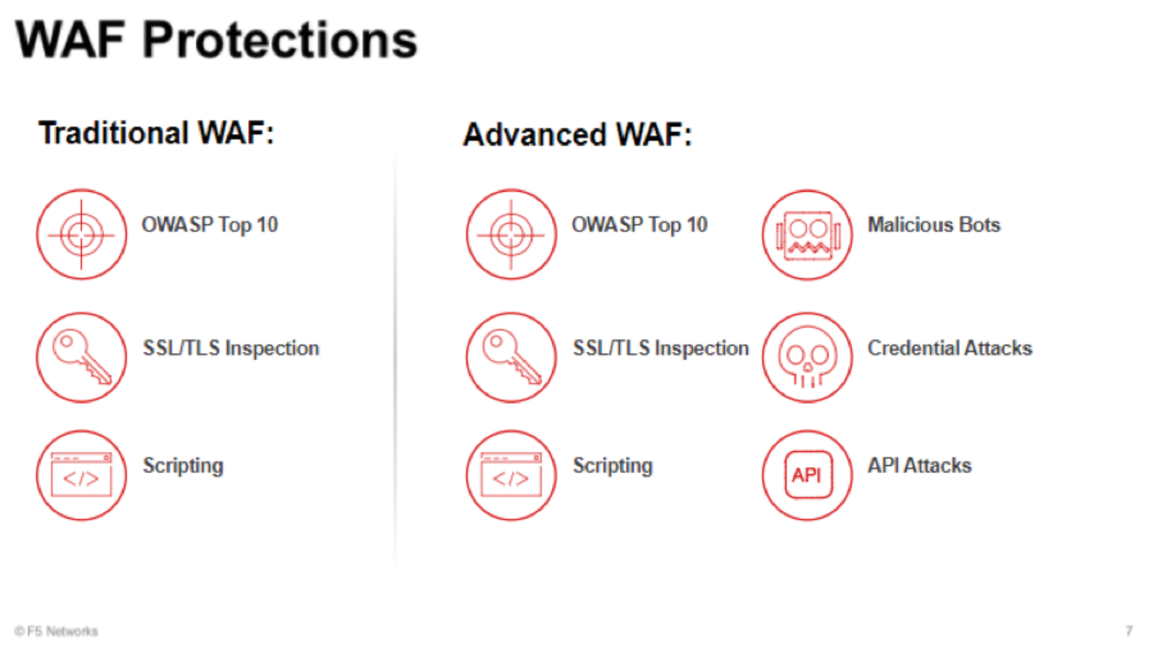
7.5 Web Applications Protection - application firewalls

Security versus functionality and efficiency conflicts. Let’s try to refute this thesis on the example of Web Application Firewall.

Currently, there are several major players on the market, i.e. Imperva, F5, Radware.

The security system of “web” applications checks the structure of the portal - directories, files, parameters, that is the content of forms, the correctness of the API (Application Programming Interface) message exchange and in addition to this - traffic character. It also recognizes attackers of the so-called web scrapers trying to copy the content of the entire website, or cause denial of service - DoS attack (Denial of Service). Fortunately, we can protect ourselves against this. There are many protection techniques in the modern WAF, including brute force, which is the protection against multiple log-in attempts, checking the IP reputation of clients, protection against frauds, interception of sessions, data leakage through for example the masking of displayed confidential data, such as credit card numbers, document numbers. The analysis of each package undoubtedly takes time, however detection and removal of unnecessary or hostile traffic, and optimization can bring much more profits.

In 2018, F5 company presented its vision of the WAF solution:



WAF Protections

Traditional WAF:

OWASP Top 10

SSL/TLS Inspection

Scripting

Advanced WAF:

OWASP Top 10

SSL/TLS Inspection

Scripting

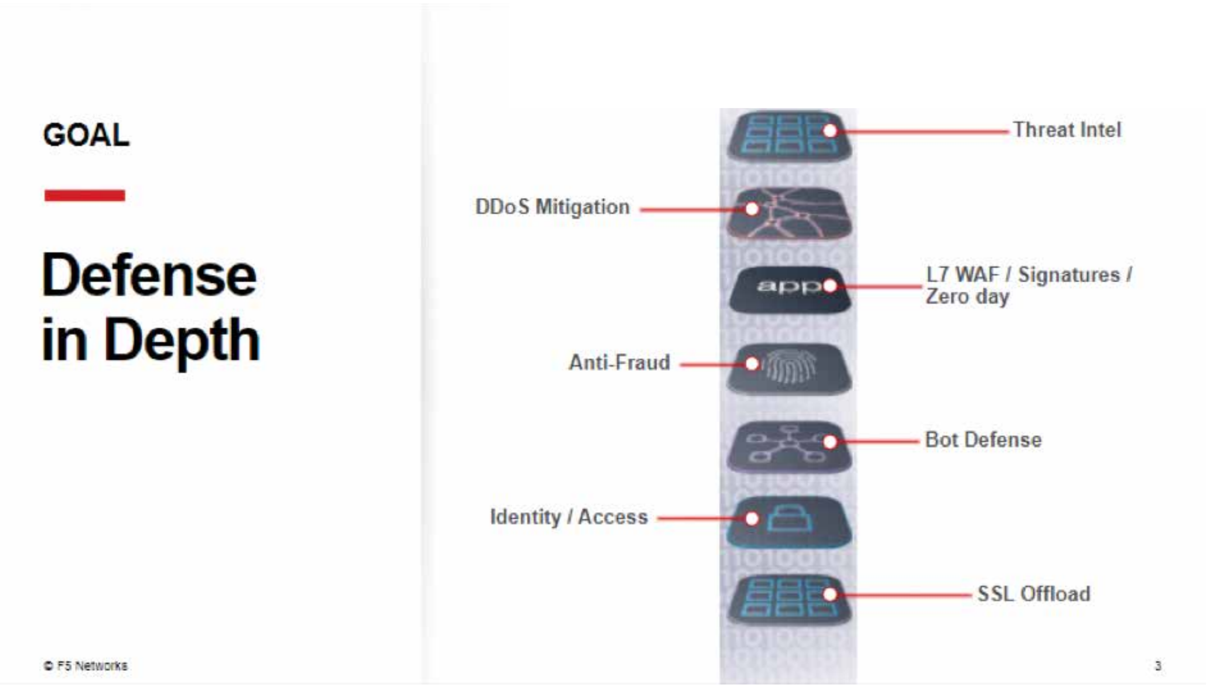
Malicious Bots

Credential Attacks

API Attacks

© F5 Networks

7



GOAL

Defense in Depth

© F5 Networks

3

The general concept of network protection among providers goes far beyond an application firewall contained in one device. It also encompasses protection against distributed, volumetric DDoS attacks and systems based on IP address reputation, honeypots, etc. Many cloud solutions are promoted. The capabilities of the Web Application Firewall alone are so enormous that we will discuss only a few selected ones here.

Let’s start with the implementation. The optimal architecture includes a reverse full http proxy with an advanced load balancer and transmission encryption. It is possible to optimize efficiency and protect on many network layers.

TCP optimization

Precise adaptation of parameters or of TCP protocol options, both from an access website and from servers’ website, whose optimal parameters may be different.

Careful selection of values of expected response time (timer) and options:

- fast open
- slow start
- selective ack
- selective nack
- Forward Acknowledgements (FACK)

can enhance efficiency of transmission, but above all it enables to avoid bottlenecks in transmissions between wide area network and local area network environments, which have significantly distinct features.

We have a strong mechanism of protection
- a SYN cookie

When WAF detects a distributed attack with the use of numerous mechanisms, it activates a mechanism, known as IP spoofing, which blocks traffic from sources impersonating false IP addresses . The mechanism effectively protects application servers from flooding the packages from distributed attacks.

SSL optimization

SSL - encryption/decryption carried out by efficient and designed for it asic or fpga hardware.

Extension of OCSP (Online Certificate Status Protocol) stapling type consists in a server adding website certificate validity confirmed by the CA (Certificate Authority). As a result, the client does not have to ask the CA about validity of our certificate. Session combination time is reduced by up to 200 milliseconds. We can notice this when opening large websites only, which have an estimated number of about 1,000 new customers per second. This way, we save about 3 minutes of the processor’s time. An additional advantage of the extension is that the client can obtain the status of a certificate even with limited Internet access. In the CyberTarcza quarantine we have such a case, in which the client has access only to the website and not to the Internet, including the CA.

Optimization of http

We can use here:

- **http compression**

  We are able to make well-adapted profiles, we can configurate according to the URL of an application or type of file content, we can also choose the degree of compression. The advantages is on the one hand the reduction of network traffic, on the other hand, relieving server processors by taking over the packing and unpacking of content.

- **cookies encryption and signing**

  The security of an application often requires encryption and authentication of cookies (http cookies). Implementing this on the central element is simple, effective and gives freedom to change application servers without the need to move data in order to encrypt between servers.

  Traffic distribution, our firewall application is integrated with the load balancer

- Loadbalance - traffic distribution taking into account the availability of application servers, their load, response times, etc.

- Oneconnect - an interesting extension that allows you to aggregate multiple TCP connections from different clients into one from WAF to the server. It diminishes the load of application server processors, exempting them from the requirement to set / close TCP connections with heavily loaded servers. The number of TCP connections to the server can be increased multiple times, even from two to four orders of magnitude, we have notable benefits that enhance the efficiency of sharing the portal.

- - http / 2 gateway is a protocol that solves the http / 1.1 restrictions and transmits many http requests in one connection. Together with Oneconnect, it significantly increases the speed of page loading, and thus eliminates bottlenecks.

Application security mechanisms

Protection of web applications is based on:

- their structure.

WAF knows the structure of directories, parameters, files. Due to its complexity, it is not easy to enter this data manually. We use the automatic learning function. A profile is created. On the basis of traffic and consultation with creators of the protected application, the security administrator decides how to treat deviations from this profile - whether as alarmed or blocked.

- the nature of the traffic, the type of a customer

WAF recognizes whether the client is a human or a machine by means of signatures, both the content of calls and their behavior, frequency of occurrence, their variability and other features, the security administrator has to select filter parameters and the way of treating the detected deviations. Analysis is a task for many teams, SIEM analysts, application administrators, and developers.

The F5 labs report shows that bot traffic in the network equals 50%-60% of the whole network traffic. Our website has a varied distribution of harmful intensity in the traffic, and can start from zero, but when there is an attack on us, cutting off non-client traffic allows application servers to do their core business, which brings the company profits, instead of losing resources on handling malicious queries or simply allowing them to work despite the attack.

The same applies to other attacks, even if servers are not vulnerable. Dedicating resources to vulnerability scanning like SQL injection, XSS or other described in OWASP A1 is unnecessary.

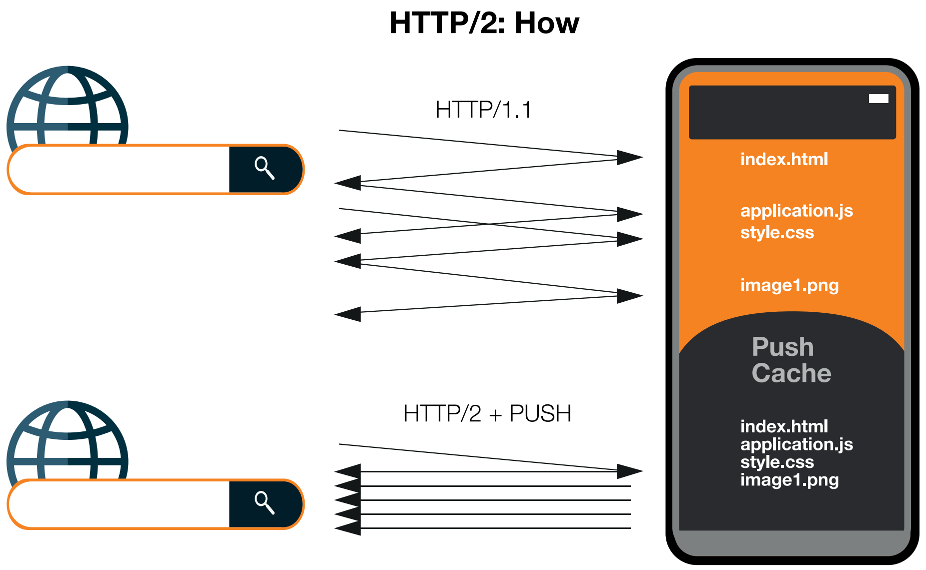


Figure 33 *Web attacks on Orange Polska mobile websites, data from December 2018.*

- brute force: protection against attempts to guess the password.

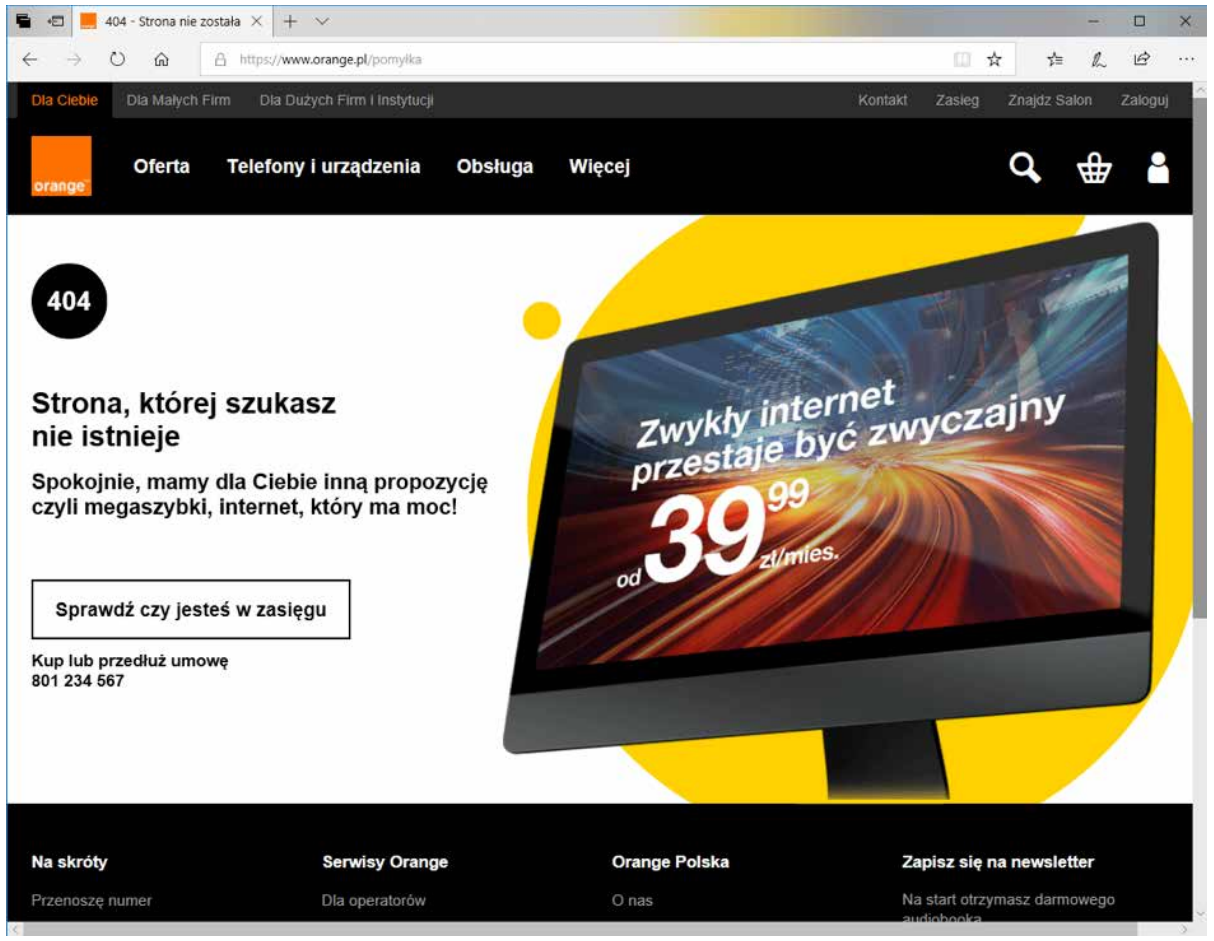
WAF can detect attempts to break log-in credentials. To thwart an attack attempt, we can disconnect, delay another attempt, temporarily block its IP, display a captcha, limit the number of sessions for a given source address or for a given client. There are more possibilities of using them. It requires close cooperation between the portal's team and security administrators, it is important to adjust the appearance of elements served by WAF to the appearance of the website.

Error handling:

In the event of unexpected server responses, we cannot share them with the client. All exceptions should be handled by the "sorry page" websites, which continue to inform about the activity of our company. Transferring it to WAF allows you to make error handling independent from changes in the application.

The above-mentioned protection techniques look perfectly on presentations of solution providers. Unfortunately, sometimes there are errors in their activity, e.g. false positive. Sometimes blocking one correct call is more costly for operators than passing 1000 malicious ones. What happens when the client cannot make purchases, because a small stroke has appeared in his/her surname, and WAF recognised it as a violation and blocked the website. We have to select security policies very carefully, but also we need to take into account dynamic changes in the web application. In the course of creating an application and implementing changes to it, its developers also have to remember to maintain security and avoid vulnerabilities.

A common belief that programmers care solely about functionality and efficiency of an application, and security engineers do nothing but limit their capabilities, should be gone forever. For optimal operation, close cooperation of many teams is needed, and their actions should always be aimed at one goal of providing the user with a reliable, functional, secure and attractive application.



404

Strona, której szukasz nie istnieje

Spokojnie, mamy dla Ciebie inną propozycję czyli megaszybki, internet, który ma moc!

Kup lub przedłuż umowę
801 234 567

Na start otrzymasz darmowego audiobooka

7.5.1 Web attacks on Orange Polska web portals

The presence of Orange Polska on the Internet is connected with complex architecture. It comes as no surprise that resources of this kind are exposed to hackers' attacks. Criminals' goal may be, for example, taking over the control of a website or gaining access to sensitive data. To prevent this, CERT Orange Polska not only reduces the risk of vulnerability occurrence on websites, but also protects them actively by registering and blocking thousands of suspicious events every month. In addition to those "classic" actions, such as injecting a malicious SQL code (which for years has occupied the first place on the OWASP TOP 10 list), cross-site scripting or vulnerability scans, we filter, monitor and block traffic on HTTP/S protocol to avoid more sophisticated attacks. In this area we use WAF - a network firewall protecting web applications.

Based on the data of December 2018, we can observe that the most types of attacks on mobile websites (more than ten thousand registered events) were based on an attempt to use the current functionalities of websites maliciously (Abuse of Functionality). Attack attempts through extracting data from web applications (Web Scraping) are also notable. We are also constantly monitoring a large number of events concerning gaining access to restricted websites or other confidential resources on network servers through enforcement (Forceful Browsing).

Number of incidents	Attack	Threat level
15936	Abuse of Functionality	"Hight" threat level
6648	Web Scraping	"Medium" threat level
2254	Forceful Browsing	"Medium" threat level
1219	Session Hijacking	"Medium" threat level
727	HTTP Parser Attack	"Medium" threat level
639	Predictable Resource Location	"Medium" threat level
526	Command Execution	"Medium" threat level
130	Non-browser Client	"Medium" threat level
127	Parameter Tampering	"Medium" threat level
122	Path Traversal	"Medium" threat level
118	Injection Attempt	"Hight" threat level
36	Cross Site Scripting (XSS)	"Medium" threat level
15	Trojan/Backdoor/Spyware	"Medium" threat level
15	Vulnerability Scan	"Hight" threat level
12	Information Leakage	"Medium" threat level
5	Server Side Code Injection	"Medium" threat level
2	Detection Evasion	"Medium" threat level

Table 1 Web attacks on Orange Polska web portals, data from December 2018.

Number of incidents	Attack	Threat level
7548	Buffer Overflow	"Hight" threat level
6046	Abuse of Functionality	"Medium" threat level
5019	Forceful Browsing	"Medium" threat level
4457	Path Traversal	"Medium" threat level
2713	Abuse of Functionality	"Medium" threat level
1467	Injection Attempt	"Hight" threat level
1204	Predictable Resource Location	"Hight" threat level
1116	Path Traversal	"Medium" threat level
1082	Remote File Include	"Medium" threat level
735	Cross Site Scripting (XSS)	"Medium" threat level
618	HTTP Parser Attack	"Medium" threat level
560	Non-browser Client	"Medium" threat level
495	HTTP Parser Attack	"Medium" threat level
414	Information Leakage	"Medium" threat level
220	Buffer Overflow	"Medium" threat level
123	SQL-Injection	"Hight" threat level
63	Command Execution	"Medium" threat level
29	Denial of Service	"Medium" threat level
24	Non-browser Client	"Medium" threat level
17	Server Side Code Injection	"Medium" threat level
16	Detection Evasion	"Medium" threat level
9	Vulnerability Scan	"Hight" threat level
2	Authentication/Authorization Attacks	"Hight" threat level
2	XPath Injection	"Medium" threat level
1	LDAP Injection	"Medium" threat level
1	Directory Indexing	"Medium" threat level

Table 2 Web attacks on Orange Polska web portals, data from December 2018.

In December 2018, most of the attacks on websites were aimed at buffer overflow (Buffer overflow). The threat resulting from this kind of events and Injection Attempt, Predictable Resource Location, SQL-Injection, Vulnerability Scan Authentication / Authorization Attacks are considered high-level threats. It has been noted that there are over 6,000 events connected with the malicious use of websites' current functionalities (Abuse of Functionality), and a significant number of events concerns attempts to gain access to restricted websites (Forceful Browsing).

Jerzy Michajłow

7.6 Artificial Intelligence and Cybersecurity – It Cuts Both Ways

#lightside

Issues related to Artificial Intelligence (AI), in particular Machine Learning (ML), have been present in the field of cybersecurity for as long as 30 years. The simplest form of artificial intelligence in the form of expert systems (yes, that is also an AI!) was the basis for the functioning of Intrusion Detection Systems (IDSs) as early as in the late '80s, and today, it can be found in SIEM systems. Machine learning (i.e. systems that are working increasingly better as they gain experience) has been used in antivirus software since the nineties, based upon the naive Bayes classifier (prediction of categories within an unknown set of data). Many modern solutions use variants of that technique, which, in its simplest form, comes down to the elementary idea of every word found in a document having a weight assigned to it that associates it with unwanted e-mails. Some words (such as "payment", "login", "invoice") are much more likely to sound the alarm than others.

Naturally, the methods used today can be much more advanced. One example are the Web Application Firewalls (WAFs), which detect anomalies as aberrations from profiles of the typical traffic generated by the website and its users that have been "learned" by the system.

Magic? Hardly!

Terms such as artificial intelligence, machine learning and neural networks sound like magic spells for solving all problems. Yet, those are ordinary mathematics, some of them more complex than others. Using the phishing e-mail classification problem as an example, we will describe what it is like in practice.

Phishing campaigns are counteracted chiefly by blocking data extortion websites created by criminals. However, in order to accomplish this, they must be identified first. This is done by various units, such as SOCs and CERTs, which analyse potential threats. Websites such as OpenPhish, PhishTank, or even Twitter, where researches from all over the world exchange information on domains used by criminals, are also a valuable source of knowledge.

However, what to do when a completely new, previously unobserved campaign appears? What to do when criminals create another website which has not been reported by anyone and the campaign samples have not reached the SOC or CERT yet? Is waiting for the first harmed users in order to identify and block the resources used by the criminals by analysing the incident the only thing we can do?

In case of new threats, AI comes to our rescue. Based on historical events, algorithms learn which traits are noteworthy and which are irrelevant from the perspective of e-mail classification. This is not just about the presence of specific keywords (such algorithms are easy to deceive), but also about such traits of the e-mail as structure, coding, construction of the URLs contained in it, and many others.

We begin the task by collecting and describing a set of e-mails to feed our algorithm. We will demonstrate this on the example of a sample of e-mails reported by employees and verified as suspicious that have been collected for training purposes. The opposite class will be comprised of a similarly sized sample of the remaining e-mails. When preparing such a set, remember to clean it – remove repetitive e-mails, eliminate erroneous data, etc. Describe each message with numbers corresponding to its individual traits:

	mail 1	mail 2	mail 3	mail 4	mail 5	mail 6	mail 7	mail 8	mail 9	mail 10	mail 11	mail 12
Subject includes: invoice	1	0	0	1	1	1	0	1	1	0	1	0
Contains DOC attachment	0	0	1	1	1	0	1	0	1	1	1	1
Contains PDF attachment	1	0	0	0	0	0	0	1	0	0	0	0
Number of links in – email	1	3	0	0	0	1	0	0	1	0	0	1

Table 3 *Phishing e-mails classification.*

Of course, in practice, the amount of collected historical data reaches hundreds of thousands of messages and there can be dozens or hundreds of traits describing each one. Graph 34 presents our set of approx. 800 e-mails, half of which are phishing e-mails. Each column of the chart is a single e-mail, and each of the 80 lines is one of its traits, such as the presence of a specific keyword, size of the e-mail, number of links contained in it, etc. You can clearly see that the arrangement of traits of phishing e-mails (gathered on the right side of the chart) differs significantly from the traits of the remaining e-mails.

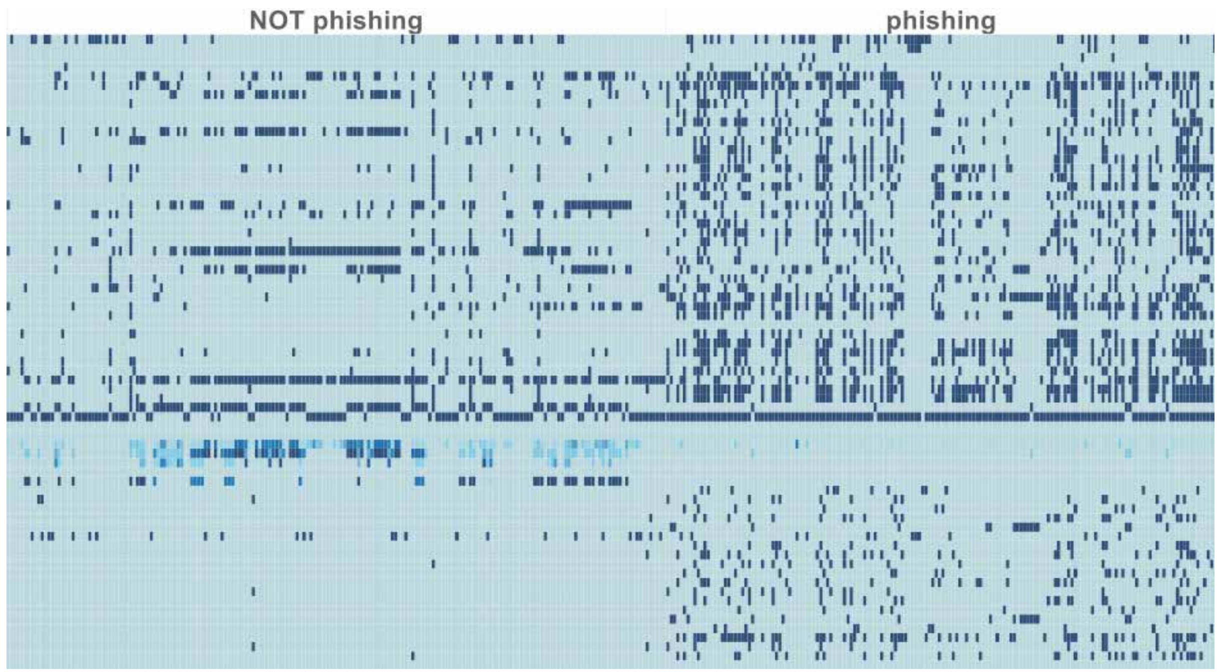
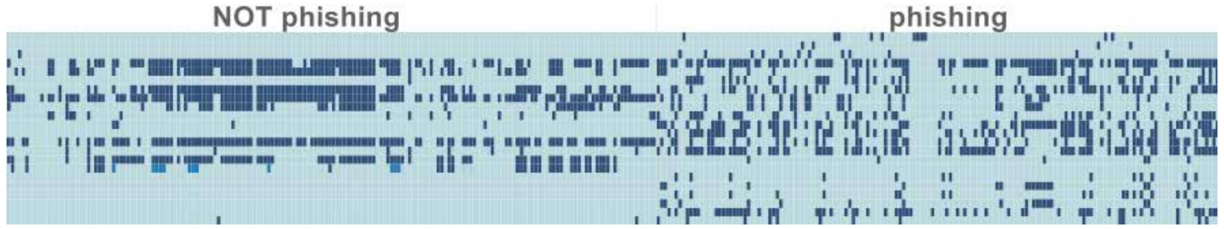


Figure 34 *Phishing e-mails classification.*



In the subsequent step of the algorithm, traits which differentiate the two sets the most efficiently are automatically selected. In the case of this set, the algorithm has decided that 23 traits are enough for such differentiation. For obvious reasons, we cannot reveal what parameters those were ☺.

In the next stage, select the model appropriate to the problem being solved and estimate its parameters based upon specific traits. The parameters are determined so as to minimise the number of misclassified elements for specific learning data (a set where we know which elements belong to which class).

The model will be used to assign new e-mails to either the phishing or non-phishing class. With an additional set of test messages, you can verify the correctness of your model by calculating the so-called error matrix, which informs you how accurate your model is. For this purpose, we have tested the model on 250 extra e-mails (in the 50/50 proportion).

In nearly 95% of all cases, our algorithm has correctly classified the test e-mails. Unfortunately, there have also been some instances of phishing e-mails being let through by the algorithm as “legit” and of genuine e-mails being considered as phishing.

No algorithm is 100% effective. The use of AI does not exempt us from the need to take precautions. Artificial intelligence provides us with serious support in the processing of an enormous number of events, but a certain margin of uncertainty of the responses received still remains. Hence human intervention is still needed for making critical decisions.

Michał Łopacki

The results of this action are as follows:

		real class	
		phishing	no - phishing
class	phishing	45,7%	1,6%
predictated	no - phishing	3,9%	48,8%

Table 4 *Assign new mails to the phishing / non-phishing class*

> ”
>
> **Deepfake will bring this type of threats to a new level. The use of deep learning will enable the putting of any words into any politician’s mouth and fiction will be indistinguishable from the reality.**

7.7 Artificial Intelligence and Cybersecurity – It Cuts Both Ways

#darkside

We often face a situation where a new solution or technology intended to make our lives easier quickly starts to provide fuel for criminals. An interesting technical example of attacks are Internet domain names containing non-ASCII characters (IDN – Internationalised Domain Name), and their popularisation in websites has led to phishing attacks where the address of a website viewed by us is often indistinguishable from the original. Check what you can see in the address bar after typing in the terribly suspicious-looking address: https://www.xn--80ak6aa92e.com/.

Another example, this time concerning the motivation behind the attacks, is e-banking and its more exotic variant – cryptocurrencies. They are beco-ming an easy target for plundering, and also allow cybercriminals to use infected computers literally as money mines. There are countless such examples.

What about machine learning and artificial intelligence (AI)?

Following the popularisation of Bayesian Spam Filtering at the turn of the 20th and 21st centuries (see [#lightside] for details), ideas on how to outsmart such systems immediately emerged.

One method is "Bayesian poisoning", which consists in supplementing the e-mail being sent with keywords strongly silencing the aforesaid "alarm". Other methods include moving part of an "unwanted" keyword (one that evidently suggests spam) to a new line, introducing a small typo into it or writing it in the form of an image. Modern spam and phishing detection systems naturally take such methods into account, e.g. they have OCR components to detect text written on images.

The modus operandi of filters based upon the naive Bayes classifier is very simple, so outsmarting it is also rather easy. Unfortunately, more sophisti-cated models, e.g. based upon Deep Neural Networks, can also be susceptible to e-mails constructed in a particularly "malicious" manner. "Adversarial Machine Learning" is currently becoming an entire separate field of research. One example which perfectly illustrates the potential threat is an attack on a traffic sign recognition system. The traffic sign "stop", properly recognised by the system, is cleverly converted into an image that is nearly indistinguishable to the human eye, but recognised by the neural network as the "give way / yield" sign (its American version has different colours than the one known in Europe).

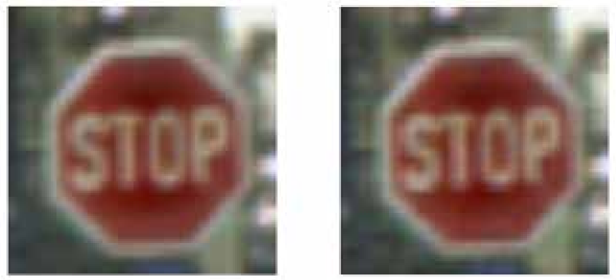
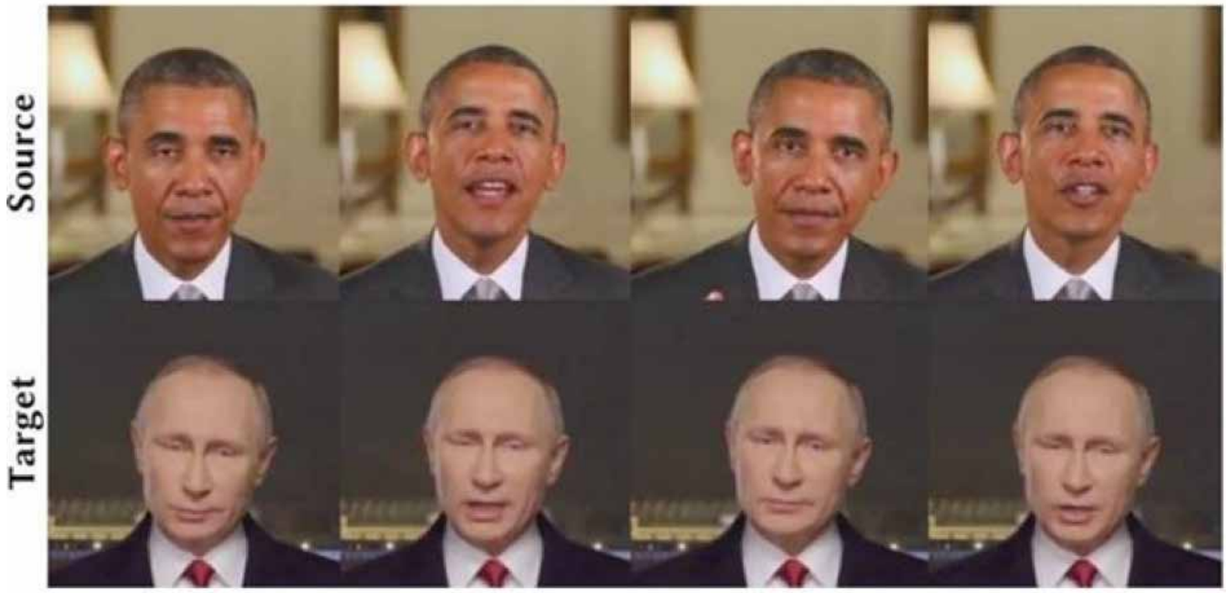


Figure 35 *Source: Nicolas Papernot, Patrick D. McDaniel, Ian J. Goodfellow, Somesh Jha, Z. Berkay Celik, Ananthram Swami: Practical Black-Box Attacks against Deep Learning Systems using Adversarial Examples. CoRR abs/1602.02697 (2016).*

Resilience to such attacks is crucial in healthcare, military, biometrics, financial, cybersecurity, IoT, autonomous vehicles, smart buildings and city systems. However, nothing remains without a response – research on the structure of "malicious examples" in machine learning also results in better understanding of how to build models and systems more resilient to such techniques.

Cybercriminals are attempting to outsmart machine-learning-based security systems – but machine learning itself is becoming a tool in their hands with increasing frequency. One example are OCR systems breaking the CAPTCHA protection, which is meant to be a Turing test restricting the influence of bots on websites.



In order to relate adversarial machine learning to the world of telecommunications security, one must mention the use of ML for the creation of a bypassing code that detects malicious code, or of tools which check it (sandboxes).

The cybernetic war aimed at destabilising the key infrastructure and economy uses malware and DDoS attacks. The information war, a special case of which is the spread of propaganda, is bound up with it. Presently, such attacks are conducted by people such as Internet trolls in the comment sections of opinion-forming portals. Deepfake will bring this type of threats to a new level. The use of deep learning will enable the putting of any words into any politician's mouth and fiction will be indistinguishable from the reality. Examples of deepfakes demonstrate how easy it is to do even in real time.

For more examples of what criminals could use ML for, see: https://www.welivesecurity.com/wp-content/uploads/2018/08/Can_AI_Power_Future_Malware.pdf – selection of targets of attacks, learning the workings of the network in order to match its own move to them and not get detected by NBADs, etc.

We cannot hope for artificial intelligence to be a panacea that will solve our problems for us. Today, it is merely a tool. This is somewhat encouraging – as we should not need to worry that it will be invincible when used for nefarious purposes. However, what awaits us is an unceasing race in which we can never fall behind.

Nevertheless, I have some misgivings about AI, concerning other issues. Setting the context of cybersecurity aside for a moment, let us note how quickly computers are replacing people in more and more aspects of life – for example, software can already create beautiful music by itself nowadays. Tying the topic of artificial intelligence to broadly-defined risk, I am also going to mention the existential risk.

We are afraid that a powerful and uncontrollable AI could create a prison in which people would vegetate like plants, just like in the "Matrix" movie. This topic was also mentioned by Stanisław Lem or Stephen Hawking. Interestingly, hardly anyone cares about the very same AI that one's would create - whether the AI would "feel" itself happy? The fear related to existential risk was also found understanding among entrepreneurs like Bill Gates or Elon Musk. The latter is a co-founder of the research organisation OpenAI, whose goal is to develop a "friendly" artificial intelligence, and he is one of the few people today who are openly advocating introducing regulations on AI.

We do not know what it will look like tomorrow, but it's worth realizing how much it all depends on us themselves. Everything we create brings with it intentions. As people, we have free will and from us it depends on where this world is going. If we want to entrust AI with any form of "free will", we have to develop it in a responsible manner. Just like parents are responsible for their children by instilling in them morality from their own parents.

Wojciech Świeboda

There are some very popular buzzwords that are ambiguous and very broad and evolve over time but are known and recognised by everyone. One such example are the terms Artificial In-telligence and Big Data. They refer to a field of knowledge called Data Science. The process of acquiring that knowledge includes Data Mining, which uses Machine Learning algorithms. Deep Learning, which uses various tools, such as Deep Neural Networks algorithms, is a special case of that. Data Science also includes statistics, data visualisation and business analytics

7.8 Malware as a Service – the Long Supply Chain of Botnets

One poisonous mushroom in a dish is enough to spoil the taste of the entire meal. That is a truism and the successful activities of Red Teams only appear to be confirming it. However, are cybercriminals attacking alone?

The answer is no.

However epic and Robin Hood-like a story of a single person facing up to large corporations sounds, the mechanics of preparation and conduct of an effective attack requires many very diverse sets of skills.

Some companies are already forecasting that over the next few years, cybercrime will have surpassed illegal drug trade in terms of the value of its generated income. Although such predictions appear slightly premature, one thing is certain – the cyberspace still remains the perfect place for crime to grow, and the future will be written online.

Especially when the goal is to maximise the pro-portion of profit to the outlays and effort put into it. Sounds like one of the principles of efficient enterprise management? Of course it does. Cybercriminals have long been employing practices analogous to those of their greatest, most profitable targets – companies and corporations.

In the market, there exist in separation and yet in mutual dependence researchers, who are seeking new vulnerabilities and attack methods; software developers and coders, turning a code into malware; botnet and management server administrators; as well as an entire group of other people; much like in an enterprise, belonging to their own analogous “departments” and project tasks.

Let’s say that Mr X intended to leave his IT job at a large corporation. As most people changing jobs, he was not satisfied with his current situation. He was dissatisfied with either his boss or with his salary and the general work climate, as well as with the monotony of his tasks. He was contacted via Linkedin by a headhunter, who arranged a telephone call with him. During the call, the recruiter, by efficiently using Mr X’s resentments, learned the name of Mr X’s boss and heard about the manner in which he interacted with people. He also learned about the structure of the business e-mail addresses of the corporation’s employees when Mr X gave him his business address as a backup address for their correspondence. The meeting ended, Mr X went home in a better mood, having vented his anger, and the recruiter told him to take care and promised to stay in touch. He had collected enough data to begin preparing his attack and already had several effective infiltration methods in mind. He could ask his software developer colleagues to prepare a discreet RAT to be placed in his subsequent message for Mr X. In order to avoid burning any bridges, his phisher acquaintances would send it at Mr X’s business address from a spoofed address, impersonating his sharp-tongued boss. Once the malware is successfully installed on the station, the recruiter will have to contact his group. They will still have a lot to do, including the slow identification of vulnerabilities, the most sensitive systems and open network communications ports, and the development of methods for effective exfiltration of the collected data to their previously contracted client.

There are many scenarios similar to the one described above. A business can start from the creation of a botnet, which can be sold or leased to a completely different group and used to conduct attacks. Those may include DDoS, click frauds, extortion and phishing, or malware that steals information and bank server authentication data. That is not all. Personal data can be sold, information on credit cards or bank accounts can be used, and the infrastructure taken over as a result of the attack can be used for various purposes, such as cryptocurrency mining, or for ransom demands after the installation of ransomware. Malware as a service is a popular and increasingly preferable service model of cybercriminals.

In the Orange network, we can observe a constant increase in the use of modular malware for infecting terminals. Emotet, Nymaim, Trickbot and Hancitor have taken over the role of malware meant for the initial infection of workstations, charging standing or one-time fees for distributing the results of the work of other creators. Everyone benefits from this. Botnet owners do not need to worry about their income and methods for generating revenue from the devices taken over, and the software owners or creators do not need to bother themselves with developing the infection methods. When selling their software on the black market, the creators of GandCrab are even offering a licence-based model, ensuring constant access to updates and support channels for their clients. This modus operandi also makes the standards for the terminology and definition of threats developed in a slightly differed period of time obsolete. After all, it is difficult to decide how to classify a binary which successively delivers to stations a banker, an infostealer and ransomware, particularly when its subsequent functions are more characteristic of Backdoors. Indeed, classifying each sample as a dropper or downloader does not fully explain the risks faced by the infected station.

The chain of people benefiting from just a single infection is impressive and the above examples are merely the tip of the iceberg. Advanced persisted threats (APTs) operate based upon an even more complex division of duties, tasks and successive lifecycles of the threat. The so-called malware supply chain is constantly evolving and seeking new methods for infiltrating its located targets.

Some companies are already forecasting that over the next few years, cybercrime will have surpassed illegal drug trade in terms of the value of its generated income. Although such predictions appear slightly premature, one thing is certain – the cyberspace still remains the perfect place for crime to grow, and the future will be written online.

Piotr Kowalczyk

7.9 Security of SOHO routers

Although the awareness of the security importance of our home gateways is steadily growing, this segment of network devices is still far from an ideal state. Over the past few years, we validated a dozen or so SOHO routers, which are on offer in the Orange company, and countless devices participating in the incidents we response to.

Client-side security

The most popular administrative interface is the one which can be accessed via an Internet browser and on which the most of aggressors' attention is focused.

The majority of the tested solutions was equipped with data filtration mechanisms transferred to the client's side, i.e. managed with the use of JavaScript. Such an approach is ineffective and fails to achieve the goal - all you need to do is modify a form using browser development tools, disable JS support, or send a request using console tools, such as cURL.

There are more contraindications to excessive reliance on client-side mechanisms. Imagine that session management is based on cookies, and the logout mechanism is executed from the level of JavaScript. When one wants to force the use of the HttpOnly flag, logging out will become impossible.

Sensitive data in an explicit form

Have you forgotten your credentials to a PPP session and for some reason you need them? It is highly probable that you will find them in the source of the administration panel website. There is also a good chance that you will be able to read them from the downloaded configuration file. These are the things worth checking at the very beginning, although the result may shatter your illusions about what you are dealing with.

Cross Site Scripting

Vulnerabilities of this kind are just as old as the first dynamic websites. They are mostly present in SOHO routers as well. One of the factors to be blamed is the aforementioned fact of data filtration entered into forms on a browser. The problem could be solved by transferring it to the server's side, but it wasn't always the case. Validation often came down to cutting out key words like "script", "document" or "write", which did not solve the problem. Instead, one was forced to search for some methods of circumventing the blacklist with the use of less known functions or exotic encodings.

Sometimes a wrong code could not be injected from the GUI, but it could be done by providing it in the form of appropriate variables in the configuration file (provided it was stored in a public form) followed by reuploading.

Injecting a code by means of the hostname field in the DHCP request to assign a new IP address (DHCPREQUEST) is an interesting vector, too. In such a situation, the code would be executed in the tab displaying clients connected to the network, which in some cases was tantamount to the index of administration panel.

Password issues

Default passwords such as "admin" or "123456" do not bring anything good, but they are nothing new, either. It is commonly known that it is better to weaken the security of a solution than to expose the client to the inconvenience of copying a much more complex password from the sticker placed at the bottom of the device, or calling a provider with a request for password reset.

It is not so bad if administrative services are not exposed to WAN, but it's not worth searching for reasonable password policies. The greatest achievement in this field was forcing one of the providers to display a message requesting a password change after logging in for the first time. Only one of the tested models actually did not allow/enable to conduct administrative work until the password was changed (sic!).

The second thing worth considering is the mechanism generating WIFI passwords (I omit the issues regarding encryption algorithms, because fortunately WEP and WPA have been dead for a long time now). Sometimes a password consisted of a fixed string and, for example, the last four SSID characters. If the owner of such a network did not change its name, it became open to anyone who was within its range.

The last issue concerns the way of sharing and storing passwords. Routers produced by a certain Polish company shared credentials in an open text, what is more - with the use of the GET method. It was a unique abnormality, but competitive companies also did not fall behind and used base64 (or bruteforceable Basic-Auth). I was faced neither with implicit password sharing nor with using the shortcut function as if they were too resource-consuming and too expensive to implement.

Communication encryption

One of the fundamental security practices should be the provision of communication encryption between administrative interfaces and the user. In reality, this situation occurs relatively seldom, which producers set down to technical parameters of after all "weak" devices.

In this way, the client receives the Telnet service instead of SSH, and instead of HTTPS - HTTP (Some models indeed had both services running simultaneously, which was contrary to providers' version, but in such a case there was no automatic redirection to the encrypted instance, anyway). Producers voiced similar arguments when attention was drawn to the insufficient key length (typically 1024 bits), although I did not manage to find results of performance tests.

On the other hand, if the traffic to GUI could be made in a cryptographically protected of cryptographic protection, it turned out that the certificate was signed personally and was thus untrusted. I n addition to this, it expired 5 years earlier (...).

Hidden Feature

Validating two devices from the same manufacturer, adaptation to work with other services made access to some functions only seemingly removed. Scripts were still in the system, and the manufacturer deleted only links to them. Unfortunately, it is a very common practice, probably resulting from hurry.

What else?

Of course there are many more gaps, but they do not appear in every second tested solution as described above. There were such gaps that resulted from bad implementation of standards or network protocols (vulnerable implementations of WPS or UPnP); memory control (buffer overflows); data transfer from the user to the shell (remote code execution), session management (auth bypass); errors in application logic (i.a. Denial of Service) and more.

SOHO routers will always be on hackers' target as a relatively easy to acquire stronghold for further illegal activity, such as carrying out subsequent attacks, building botnets, etc. That is why, their software should be periodically tested for security

Conclusions

As one can easily observe, one thing stems from the other, creating this way a chain of deficiencies in security. SOHO routers will always be on hackers' target as a relatively easy to acquire stronghold for further illegal activity, such as carrying out subsequent attacks, building botnets, etc. That is why, their software should be periodically tested for security. The ubiquitous fashion for "IoT" is the reason for us having a lot of interesting research and at the same time plenty of cases of neglect in security.

Kamil Uptas

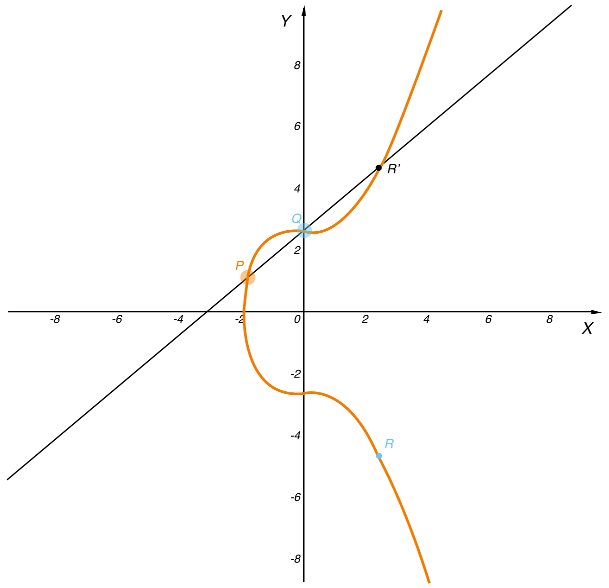
7.10 Bitcoin – a case study

The world of the blockchain technology and cryptocurrencies is developing at a very fast rate. Bitcoin, which was the first to be developed, enjoys the most popularity. For this reason, it also attracts cybercriminals' attention.

In this article, we will take a look at bitcoin's security, and two methods employed by cybercriminals to steal the digital currency (Focusing on how the network works, not on the subjects using Bitcoin – such as stock market etc.).

To understand the mechanism of creating addresses in bitcoin, it may be good to look at how creating a public key using elliptical curves works. A curve of this kind is shown below (with points):

$$y^2 = x^3 + 7$$

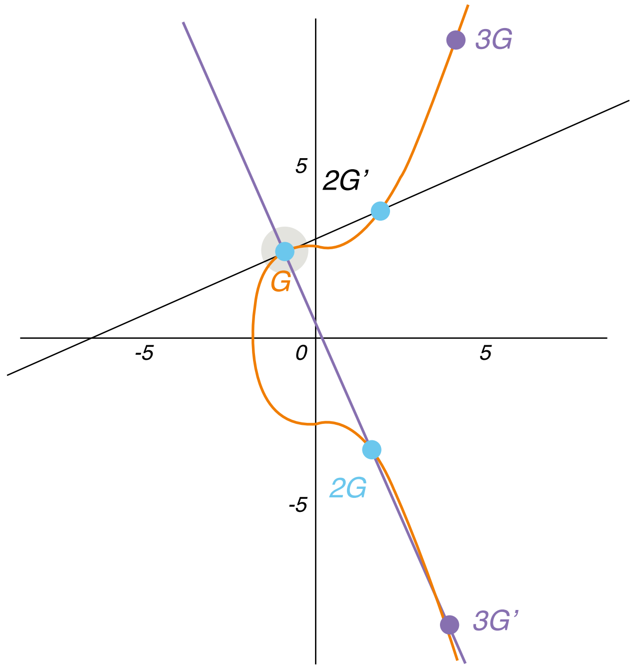


While calculating a public key, two operations are used; adding a point, and doubling it. To add points P and Q we need to draw a line through the points, and the intersection with the curve (beyond that two points) is point R', which after being projected onto the X axis gives us point R.

Doubling a point (e.g. G point of origin) consists in drawing a tangent through that point, and the common point of that tangent and the curve, represents point 2G', which after being projected onto the X axis gives us point 2G.

The private key is a large, randomly generated number (256 byte), which is then multiplied by the G point of origin used by bitcoin – the result is the public key, meaning X and Y coordinates. The key may be represented solely using the X coordinate (compressed public) – the Y coordinate can be calculated.

As an example, we will break the rule of creating the public key as a large random number – we will assume that it is number 3. We will create a public key using that number:



That is what the process of creating a public key using elliptic curve in the range of real numbers looks like in a nutshell. In the case of the curve used by bitcoin, the curve is calculated in a finite field which represents a large prime number: $p = 2^{256}-2^{32}-2^{9}-2^{8}-2^{7}-2^{6}-2^{4}-1$, so the result of every calculation must into this range. The representation of the points will look different – it will consist of randomly located points symmetrical to the X axis, while the equation will look like this:

$$y^2 \text{ mod } p = x^3 + 7 \text{ mod } p$$

In the case of large numbers, it is extremely difficult to obtain the private key while knowing only the public key. Currently, the only known method is searching the entire range, which takes a lot of computing power and time.

Elliptic curves are not used for encrypting anything in the blockchain, but to prove the "network", that the emission of a transaction is actually initiated by the wallet's owner – through a digital signature. A wallet is actually nothing but a private key, from which a public key is obtained, and from that an address (or rather a pair of addresses, a compressed and uncompressed one – we exclude P2SH and segwit addresses here). Below, the process is presented in a chart form:

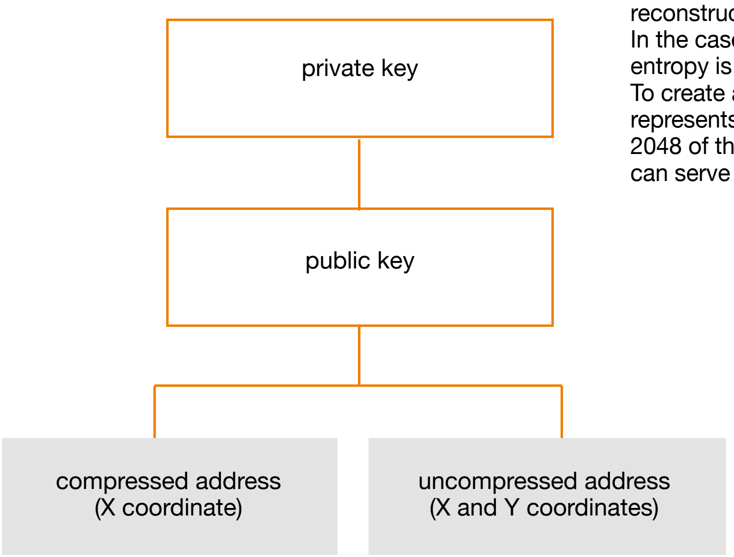


Figure 36 Process of creating Bitcoin's public key and addresses

The process of creating a compressed and uncompressed address (the only difference is in the point 1):

1. Sha256(02 + X) lub Sha256(04 + X + Y)
2. Ripemd160(1.)
3. 00 + 2.
4. Sha256(3.)
5. Sha256(4.)
6. 3. + 4 pierwsze bajty 5.
7. Base58(6.)

As an example – a private key being a SHA256 hash of the word "secure" gives the following coordinates:

X: 33fef0a65b8d3dc5941d31e0a40ee4de32b59204ff37ec601750796f59dafb53
Y: 069997cd8badd15f862626c5a8d8859dbeed5b65da43bf9968469f99d372c46c

And its addresses are:

– uncompressed:
1CvTyRmJZ19gYUK4bUdmPX843oAmN3TZLF

– compressed:
1AjJJHqa1sEvPWyMee6XCarxAgpRBpHmdG

Brainwallet

In the deterministic wallets (introduced in BIP-32), keys are created basing on the main key (seed). The BIP-39 document defines the creation of this kind of seed and its representation as a pattern – a set of mnemonic words. This kind of wallet is more easily remembered, it is more orderly then a random wallet, but most of all, the reconstruction of the seed allows restoring all the keys. In the case of the last generation of deterministic wallets, entropy is similar to private keys generated randomly. To create a secure wallet, a seed is generated which represents 12 (and more) random words from amongst 2048 of the available ones (defined in BIP-39). Later it can serve to create one or many wallets.

Brainwallet is a version of a mechanism similar to the deterministic wallet, which works very simply: basing on data entered by the user, hash SHA256 is created and used as the private key for the wallet – subsequent wallets can be created by adding further numbers to such a password, e.g.: secure1, secure2 etc. Because of this, the security is significantly decreased. Firstly, because the possibility of creating a wallet based on a short and simple password, secondly, because the creator was human, which can result in commonly used words to be utilized. A brute force attack attempt on a private key SHA256 may lead to the interception of assets on a given address. One can get interesting results by creating a private key through hashing such passwords several times, or using a different algorithm. The number of wallets on which transactions have been performed can be counted in thousands.

Examples of such wallets are presented in the table below:

Signature pattern:

$$S=k^{-1}\cdot(m+R\cdot d) \mod n$$

Where:

S – signature
k – temporary private key
m – entry hash
R – temporary public key
d – private key (of the address from which the transaction is being emitted)
n – large prime number used by bitcoin

In the signature, S and R values are added, and the network verifies the signature by adequately calculating entry hashes and these two values – if the result is value R, it means that the transaction has been correctly signed and accepted.

Address	Total Received	Current Balance
14NWDXkQwcGN1Pd9fboL8npVynD5SfyJAE	501.06510751 BTC	0
158zPR3H2yo87CZ8kLksXhx3irJMMnCFAN	30.28147684 BTC	0
1CLq46YiBtXy7N3nCbKYm4hsJm4Z3Gyqvg	7.33 BTC	0

Insecure signatures

Transaction is a process of moving certain assets from one address to another. Transactions are permanently written in a blockchain, and anyone can have a look at their details. To generate a transaction, and for the network to accept it, the person originally emitting it has to prove that he or she is the owner of the wallet from which the assets are being sent. For that purpose, a digital signature is used. The data being signed is entry hashes, meaning exits of other transactions directed at that address. The signature formula:

The k value should be random and never repeat. If this is not the case, then two signatures of the same address with the same k value will allow calculating the private key from an equation with two unknowns – k and d. Assuming that we have the S_1, S_2, m_1, m_2 and R values, we can generate an equation like this:

$$d=(S_2\cdot m_1 - S_1\cdot m_2) \cdot (R\cdot(S_1 - S_2))^{-1} \mod n$$

Even though transactions of this kind happened in the past and ended in loss of assets, and errors in signatures have been known for years, they were also generated in in 2018, and allowed recovering private keys to 3 addresses. In the year 2018 small payments have been sent to 7 addresses, transactions which allowed calculating the private key in the previous years.

Surely, sending assets to an address of which the private key can be easily calculated will result in losing them in as little as a couple of minutes.

Below is an example in Python, for the address 1CvTyRmJZ19gYUK4bUdmPX843oAmN3TZLF (the address mentioned above, for which the private key is a SHA256 shortcut of the word "secure". The data is an example):

Bitcoin is a relatively new technology, which is still being perfected. While benefiting from its advantages, we should always consider using the newest software version, since wrong implementation leads to the wallet being taken over.

```
>>> import ECC
>>> r = 0xc0eb253af8f097edb495e7406d22b0d141b4b80b689d378ed00d611fe8e915ae
>>> m1 = 0xee70560dd3e23bc28305804f9bdccd4fe5c11c6a35fbc609284403c9e55b981f
>>> m2 = 0x5898271f5a5528ee905880c2b841ab04c614e1ffd5c906392401bcb6ed2b414a
>>> s1 = 0xbac63ae591bf35e0c02b17215f7eb37452eef70c46428dca2f4c94dcff19e538
>>> s2 = 0x2cfd1a89214ff6b9f8134875c917071b21e348acb303c5826cf128cc734d6675
>>> n = 0xfffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd0364141
>>> private = ( s1 * m2 - s2 * m1 ) * pow(r * (s2 - s1), n-2, n) % n
>>> #check
>>> P = ECC.ec.calc(private)
>>> print ECC.BitAddress().getAddr(P.X, P.Y)
1CvTyRmJZ19gYUK4bUdmPX843oAmN3TZLF
```

Errors like that happen mostly because of wrong implementation of the signature, e.g. by generating random numbers with a seed that may be repeated. Currently the signature in the newest wallets is created using a random/deterministic mechanism, which generates a random number based on the data from the transaction. Thanks to that, the variable will always be different.

Summary

Bitcoin is a relatively new technology, which is still being perfected. While benefiting from its advantages, we should always consider using the newest software version, since wrong implementation may lead to interception of the wallet. While creating a system based on blockchain, it is also important to ensure secure implementation of vital security mechanisms. Of all the vulnerabilities, only some have been presented here. Luckily, their current range is minimal, but they are still regularly monitored by cybercriminals.

Adam Pichlak

7.11 Digital television security

What is that anyways?

“I sign an agreement, and get hardware from the provider. Sometimes it’s just a tuner/decoder, and sometimes they also add a chip card. If I eject the card, there is no image. If I forget to pay, there is also no image, even if the card is inside.”

This is how much a typical user of a decoder would know, or to be exact, an STB (Set-top box) device.

I’ll try to explain how it works, focusing only on key aspects connected with security, without touching upon the matters of emission, image and sound codecs and medium of transmission. Details can be found in the ISO/IEC 13818 standard and DVB (www.dvb.org). It doesn’t matter what way does the provider transmit the signal: whether it’s DVB-T (ground), DVB-S (satellite), DVB-C (cable) or whether IPTV is based on a Conditional Access System (CAS).

The way CAS works, is that there are encrypting tools on the sender’s side, the so-called Scramblers. A Scrambler encrypts the digital audio/video image using the CSA algorithm (Common Scrambling Algorithm), sometimes slightly modified one (concerns the BISS system). After coming through Multiplexer, an image encrypted that way is transmitted using a medium of choice to STB, where it is decrypted. CAS also serves for protecting keys used for image decryption, and for controlling privileges on the STB/card. The key used for decrypting an image encrypted with CSA is called Control Word (short CW) with a length of 64bit, of which only 48bit of is not known.

How does STB/SmartCard know what and how to decrypt?

It can be seen that communication in e.g. DVB-S technology only goes one way, meaning towards STB. For this reason, any unusual operations such as resetting the PIN code or reactivation are conducted by the client via phone or a special website, instead of being automatically issued via STB. Here, two more key terms come in: ECM and EMM.

EMM - entitlement management message – using these instructions the CAS system manages the card/STB. Because EMMs are usually visible for all subscribers, we can divide them by the number of target recipients of a single instruction:

Global EMMs, directed to all recipients at the same time – this is the way in which e.g. firmware updates are being sent, or deletion of old privileges to free up card space.

EMMs for a group of cards – through this channel, usually cyclic information is sent, such as privilege updates and CW decrypting keys for the upcoming month. A group usually includes up to 255 cards. Unique EMMs – directed to cards/STB with a certain serial number. Through this channel, usually package changes, billing-related blocks, and activation instructions.

ECM - entitlement control message – using these instructions, the encrypted CW is sent to the STB/card. ECM is being sent to the card every ~7-20 seconds, depending on the channel. CW is decrypted from ECM with a key introduced before by EMM, if the package and date of privileges allow watching the channel from which we receive ECM.

As for curiosities that may be worth mentioning – how does it happen that there are no breaks in the image, if the CW is only working for a few seconds? The card has to decode them from ECM, but the image appears immediately after entering the channel.

Each ECM contains two encrypted CWs, a current and a future one. As an example, ECMs on the channel X are being sent every 10 seconds, meaning that the CW changes every 10 seconds. We have 4 random CW keys in 40 seconds (1-4). The first ECM upon entering the channel contains keys CW (1) and CW (2), the second until 10 seconds CW (2) and CW (3), in the subsequent ones CW (3) and CW (4) etc. Thanks to this kind of construction, there is always a security buffer which ensures fluent STB image even if delays of decoded CWs to the descrambler in the STB occur. Such delays often occur when the card processes EMM or performs a second reading of permissions. Then, CW is decoded from ECM with delay.

The picture presents the logic behind the mechanism described above:

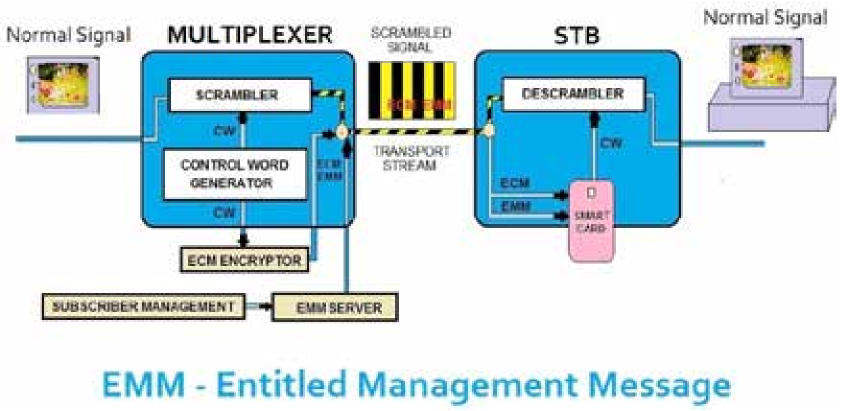


Figure 37 Picture source: https://www.headendinfo.com/ecm-emm-ca-system/

By sending EMMs to a card, the operator properly configures it, assigns permissions for channels for the upco-ming month and sends keys for decoding CW from ECM. If the card is properly configured, CWs can be decoded and sent to the descrambler. If it’s not, is sends the code of error to the STB, which is transformed into a proper error message. The user then calls the customer support to report it, and the operator finds out what went wrong. Usually in such cases card is reactivated, which means sending all EMMs configuring the card. The user is asked to change to a certain channel.

What’s the matter with this switching thing?

STB should be changed to a frequency with the highest EMM bitrate, and on which the reactivation EMMs appear most frequently. Thanks to that the reactivation process will be faster. Then why does it still take so long? Let us count how many customers each provider has, and assume that every subscriber card should receive all the permissions within an hour at most since having been switched on. These are hundreds of thousands EMM instructions blocking the band, and only the ones concerning a certain card are filtered and sent to the.

This way the card/STB knows if it can decode a certain channel.

Some of the history from CAS security measures from Polish television providers

In the beginning, there was analogue… and simple line-switching in the PAL system. It was the Nagravision System and sound modulation. Image decoders for PC were created in no time. They worked in such a way, that software was run on a PC possessing a TV tuner, which after reading and decoding the keys with an appropriate filter, it configured the lines in PAL and sound.

Figure 38 Picture source: *https://pl.wikipedia.org/wiki/Nagravision).*

Later, digital television appeared in Poland (year 1998), and security moved onto a completely different level. Sound and image would be protected by the CSA algo-rithm, and CW sent in ECM. At that time, two digital television providers emerged in Poland. First of them implemented CryptoWorks (created by Philips), and the other implemented the MediaGuard system, commonly called Seca (created by SECA) – both were broken relatively fast. They were the first ones, and rather unprepared for the fact that someone may thoroughly test them. In their case, the CW decoding keys were extracted from the ECM using modified card instructions, and with the use of reverse engineering, the entire ECM decoding algorithm was reconstructed. Soon after, the third operator appeared, who protected CWs using the Swiss Nagravision system (created by Kudelski Group), which was also quickly broken for similar reasons.

With the possession of the entire algorithm and key, a hardware emulator of such system could be created. “Zielonka” was a popular one in Poland, consisting of an eeprom and a PIC microcontroller. It had the CAS system algorithm installed, as well as keys (extracted each month from the original card or from an intercepted transmission) added using the Phoenix programmer. Emulation could also be performed on the operator’s original STB, but with programmed, modified, or alternative software. Also, makeover DVB receivers running on Linux and equipped with an Ethernet port (STB D-Box2). The capabilities of these STBs were limited only by the imagination of plugin and software developers. They were quite popular, because they didn’t have the limitations of the operator’s STBs, e.g. they could freely copy any decoded recordings from the STB or streaming live image from any channel, through SCISI(D-Box) or LAN(D-Box2) and LPT (Pioneer) networks. Another important thing was the option of using “multicam” (dbox1 interface CA), meaning cards from different CAS systems, and a CI module standard was introduced.

In 2002, Polish operators merged, and resigned from the CryptoWorks system. In the wake of the first version of the MediaGuard system being broken, the operator begun to change the system into the second version. It is important to stress that it is not possible, or at least it wasn’t at the time, to patch a CAS system in a way that would prevent unauthorized reception, and it had to be completely replaced.

In addition, the same versions of the CAS system sold to different operators usually only have different key sets and minor differences in algorithms. Breaking a certain version of the system of an operator in e.g. Spain will cause the to happen in Poland. It is only a matter of time. In 2002, cards emulating MediaGuard 2 cards of Spanish and Italian providers appeared on the market and in 2004 a software emulator of the Polish operator's MediaGuard 2 system. In 2005 Nagravision was changed to version 2 ("Aladin"), but it was very quickly broken abroad, and soon after in Poland, and emulated on the so-called "Funk" cards (processor AT90S8515 + EEPROM).

The creators of the CAS systems in versions 2.x secured their systems from being broken by introducing the option to define the algorithm decoding CWs from the ECM while the card was in the possession of the user. The algorithm could be modified through sending EMM instructions updating the card's firmware, or through a change in ECM which defined the settings of the CW decoding algorithm. In the beginning the effects were poor, because every algorithm modification resulted in updated emulators being relatively quickly released. In the end, the MediaGuard 2 platform put an end to the functioning of the emulators, probably by using an algorithm from the card's hardware, instead from its memory, or at least that's the information which appeared on internet forums at that time. Unfortunately, in case of Nagravision 2 the emulation could not be prevented due to the system having been worked out in detail. It seems like if it is not possible to reverse engineer as system, then the system is safe. Nothing could be further from truth, and this is where another important term comes in:

MOSC – (Modified Original Smart Card) – meaning the operator's original card with modified content. Usually MOSC allowed upgrading privileges or capturing/installing EEPROM.

In the first versions of systems, the card could be modified using just instructions sent to it. In further ones, the card was protected from that using cryptography, and the key was in possession of the operator or the system's developer. This is why standard modification was performed only through official EMMs. Then, how to force the card to accept an instruction if one doesn't have the key? Devices bearing a mysterious name "unlooper" appeared on the market. Their function consisted mostly in forcing the card not to perform some checking function. They would trigger a certain glitch on the card, regarding frequency or voltage at a certain time and duration while the instructions were being sent. The aim of such operation was destabilization of performing a checking function, so that the card accepted an instruction created manually, without the operator's secret keys. This allowed to e.g. to add higher privileges for another month, keys etc. or accessing data from the card's i eeprom memory.

In 2006 two new big players entered Polish market. One of them was using the Viaccess ECM system for security (created by France Télécom), while the other one the Conax system (created by Conax AS). They were rather immune to breaking, at least Conax was.

Once the security prevented further system emulation and modification of access cards, the so-called sharing was used for increasing access to content.

Figure 39 *Provider emulation cards.*

"Sharing" consists in using one or several operator cards for decoding CW from ECM, but in a client-server architecture. The card is inserted into a server with appropriate software installed and a card reader, while the unauthorized recipient connects through IP. The customer's device may be e.g. an STB running on Linux. It connects with the server with the operator card inserted and communicates with it in order to decode ECM. Assuming that ECMs on the given channel are being sent every 7-10 seconds, and the CW returns to the customer in around 400ms, this allows watching 17-25 different channels on a single card at the same time. One can easily imagine losses caused by such proceedings.

Every action causes an adequate reaction. The first one was replacing the old system with one immune to MOSC. In 2008 replacing cards and systems (Nagravision 2 to Nagravsion 3, and for the other operator, cards MediaGuard 2 to MediaGuard 3) was finished. In practice, it was the first tunnel system in Poland, which did not require replacing CAS in the receiver, but simply tunnelling the instructions to the Nagravision system. The customers only had cards replaced, without replacing STB. This kind of move was possible because in the year 2004 the Kudelski Group took over the competition, meaning it bought the MediaGuard technology from its former owner Thomson's Canal+ Technologies.

There was an additional security measure called "pairing". It consisted in the communication between the STB and the card being protected cryptographically secure. The card could be only used in the official STB, and not in e.g. a sharing server. The first version of pairing was already used Nagravision, but that one was quickly broken. The key needed for decoding the transmission resided in the STB's flash. A similar situation took place in the Conax system. Initially after implementing pairing, the system was considered to be secure, but after some time, a way was found to extract the RSA key needed for decoding CW sent by the card from the STB's flash.

The developers' next move was the ECM/CW meter. In this case, the cards were able to determine whether they're being used by a single or by many users, and thus limiting the number of channels that could be watched at the same time to e.g. 3. If that number was crossed, the card would begin sending false CWs – it wouldn't display error messages, but the image would simply not be decoded. The user had to wait a certain amount of time for the ECM to be normally decoded again. More detail on how it all worked can be found in the web, in the documents sent to the American Patent Office by "NagraCard SA".

The next, rather significant step to prevent unauthorized reception was moving the pairing keys from the memory to the processor. It was commonly known as hardware pairing, or "Chip Pairing" - great move. Unfortunately, the operators did not decide in favour of replacing a significant number of sets to the secure ones, probably because of high cost of such operation. They would only hand them to new customers, so the substitution was gradual.

Year 2012. At that time, all operators begun to equip their new customers with cards paired with decoders. These were systems such as Conax, Nagravision and Viaccess. It seemed like unauthorized reception would gradually become blocked, but there was a small false start. Researchers from the Security Explorations Company discovered an error in implementation of the pairing keys in the register of chips from the Stmicroelectronics Company, and thanks to that, the company could quickly correct that mistake. They did not publicize any details of the attack, but it was known that the POC was conducted on an STB of a Polish operator in the Conax system.

Since that time, the matters concerning TV security in Poland have not changed so much. The old hardware and algorithms, vulnerable to depairing are gradually being removed from the market, rplaced by STBs offering e.g. receiving UHD channels. Also, cardless STBs begin to appear, in which the Smart-Card's functionality has been moved to the inside of the STB. Currently, solutions like that are considered to be secure.

What awaits us in the upcoming years?

Moving the whole CAS to the inside of the decoders, and basing security on the solutions developed by hardware manufacturers collaborating with CAS providers. Apart from protecting the access to communication, CAS created an additional economic-formal barrier when it comes to access to hardware. On one hand, we have an integrated system devoid of outside communication. On the other, we have the possibility of enumerating the whole system, and increased costs for the operator, connected with the renewed need to secure the content in case the system is broken. Over 20 years of history concerning the security of multimedia content teaches us that it is only setting of another barrier, and postponing the unauthorized access.

Yet another problem is PPV streaming of channels and events. The last few years brought a significant increase in the speed and access to internet. The users no longer need a TV with a tuner, because the receivers have now become PCs and phones. Currently, the biggest problem the CAS providers have, is securing content on the internet. This is especially difficult, because in this case, the provider doesn't have a secure receiver or a card with permissions on the customer's end, but rather a standard browser or a smartphone, which is under total control of the user.

Arkadiusz Zembrowski

7.12 Cloud Security

The definitions of sources, where to look for them, and the share of responsibilities between the Cloud Providers and Cloud Customers.

Basic definitions

The definitions presented by the National Institute of Standards and Technology (NIST) in “NIST SP 800-145 - The NIST Definition of Cloud Computing”, published in 2011, are the most popular and commonly used (CSA, ISC^2 czy ISACA) The document defines the term ‘cloud computing’ as follows:

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks,servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction .

We often hear people say:

- “cloud computing does not require the use of the Internet”,
- “cloud computing is a new technology”

The fact that cloud computing requires Internet access is included in the first part of the definition: “ubiquitous, convenient, on-demand network access”. Furthermore, the definition presented by the NIST speaks of a new model of provision of IT services for business, instead of a new technology.
It is difficult to say that server or network virtualisation is a new technology.”

The NIST SP 800-145 standard describes the cloud model by:

- five essential characteristics,
- three service models,
- four deployment models.

In the graphical form, the services have been characterised below, in Figure 40.

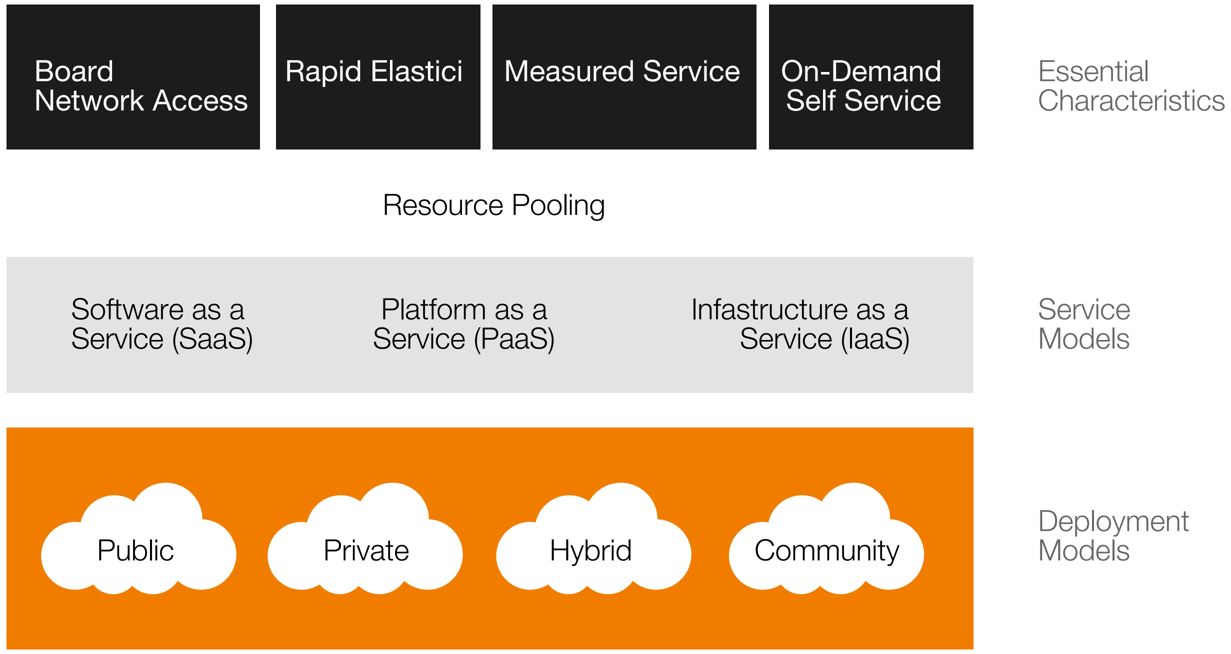


Figure 40 *Cloud model visualization presented by NIST*

The essential characteristics of a cloud are defined thusly:

- On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- Resource pooling. The provider’s computing resources are pooled to server multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter).
- Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly out ward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
- Measured service. Cloud systems automatically control and optimise resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilised service.

The above characteristics can easily be used to determine whether a service is cloud-based or not.

The essential characteristics of cloud computing enable differentiation between a Cloud Provider and a Managed Service Provider. In the case of a Managed Service Provider, it is the customer who dictates the technologies and operational procedures; and vice versa in the case of a Cloud Provider – the Cloud Provider dictates the technologies and operational procedures. The last characte-ristic – Measured Service – enables measurement at a certain level of abstraction. This s worth examining using the example of availability measurement. Traditionally, availability is calculated in accordance with the following formula:

$$\text{Availability} = \frac{\text{Uptime}}{\text{Uptime + Downtime}} \%$$

In the case of cloud services, we can sometimes see the following availability formula:

$$\text{Availability} = \frac{\text{sucessful requests}}{\text{total request)}} \%$$

Let us assume that the Cloud Provider’s system offers 99.99% availability. The first formula indicates that the system may be unavailable for 1.01 minutes per week. In the case of the other formula, let us assume that the system processes 10 million requests per week. In order to maintain the 99.99% availability, there can be no more than 1000 unsuccessful requests per week. Is a system user really going to perceive the system availability as 99.99% if most of those unsuccessful requests concern them?

The four deployment models of cloud services are often difficult to differentiate. NIST SP 800-145 defines them as follows:

- Private Cloud. The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of them (owned by the organisation, managed and handled by an external company), and it may exist on or off premises.
- Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organisations in the community, a third party, or some combination of them, and it may exist on or off premises.
- Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider.
- Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability.

In the current market, there are many providers offering Private SaaS services based upon public IaaS services: Amazon Web Services (AWS), Google Cloud, and Microsoft Azure. The question to ask is as the following: Is really Private SaaS solution or not? The definitions presented above indicate that it is not:

- a Private Cloud,, as the solution is based upon an IaaS public service, which contains the data and services of other customers, and the cloud’s infrastructure is not made available for the exclusive use by a single organisation,
- a Public Cloud, as the SaaS service itself is not

public, but meant for a single organisation and the provider of the SaaS service does not own the infrastructure,

- a Community Cloud, as the cloud's infrastructure is not made available for the exclusive use by the specific community of the organisation,

The conclusion is that SaaS services based upon public IaaS solutions and dedicated even to a single organisation should be called Hybrid SaaS. The nonchalance in the terminology may result in asking of unwarranted questions, incomprehension and unnecessary waste of time at the stage of the solution security assessment by the client.

In order to broaden one's knowledge of cloud service models (IaaS, PaaS, SaaS) and deployment models (Public, Private, Community and Hybrid), it is worth familiarising oneself with the following standards:

- NIST Special Publication 800-146 - Cloud Computing Synopsis and Recommendations
- NIST Special Publication 500-292 - Cloud Computing Reference Architecture
- Division of Responsibility by the Type of Cloud Service

Share Responsibility for Cloud Security

The most popular and commonly used (CSA, ISC^2 czy ISACA) division of responsibility for cloud security has been presented in a preparation handbook for the Certified Cloud Security Professional (CCSP) examination – The Official (ISC)^2 Guide to the CCSP CBK 2nd Edition, written by Adam Gordon, and is as follows:

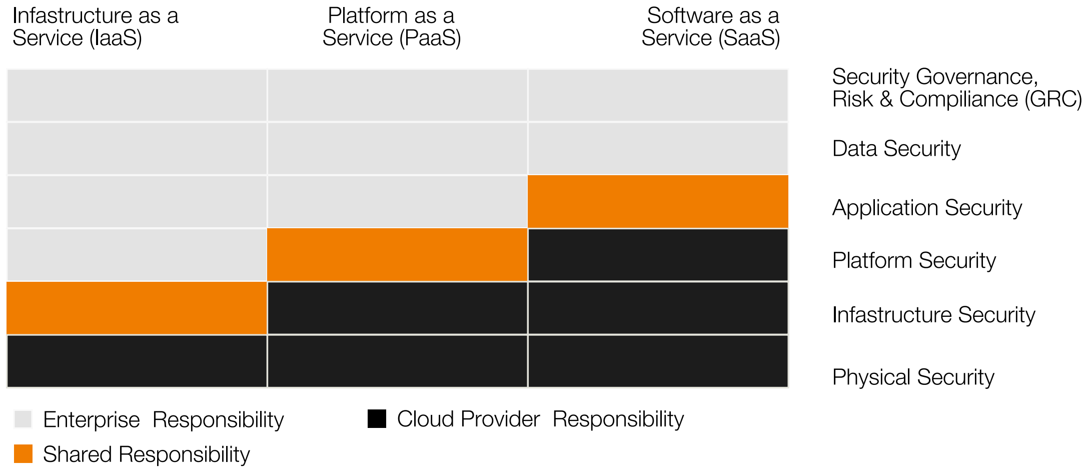
Responsibilities have been made dependent upon the service model, where:

- SaaS - Software as a Service
- PaaS - Platform as a Service
- IaaS - Infrastructure as a Service

The Cloud Customer is always responsible for the governance, risk & compliance, as well as for the data security, whereas the Cloud Provider is always responsible for the physical and environmental security.

- SaaS: In addition to being responsible for the governance, risk & compliance, the Cloud Customer shares responsibility with the Cloud Provider at the application security level. This applies chiefly to the aspect of identity and permission management (the Cloud Customer determines how many users there will be and who has what kind of access to the application). The Cloud Provider is responsible for the other levels and generally makes decisions on the manner of processing and implementation of specific safeguards.
- PaaS: In this case, the Cloud Customer is responsible for the governance, risk & compliance, as well as for the application security and shares responsibility with the Provider at the platform level. This applies chiefly to the aspect of identity and permission management (the Customer determines the programming languages, how many users there will be and who has what kind of access to the database). The Provider is responsible for the security at the infrastructural level and for the physical security.
- IaaS: The Cloud Provider is responsible for the physical security of the infrastructure and shares the responsibility for the infrastructural security with the Cloud Customer. The Customer is responsible for the security at the remaining levels. They decide what operating systems and databases are used, how many users there will be and who will get what kind of permissions.

In order to broaden one's knowledge of cloud security, in addition to the aforesaid NIST standards and the publications preparing for the Certified Cloud Security Professional (CCSP) certificate recommended by the (ISC)2, it is worth familiarising oneself with the materials available at Cloud Security Alliance's website: https://cloudsecurityalliance.org, where one can find documents such as Security Guidance for Critical Areas of Focus in Cloud Computing v 4.0[2].



	Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
Security Governance, Risk & Compliance (GRC)	□	□	□
Data Security	□	□	□
Application Security	□	□	🟧
Platform Security	□	🟧	■
Infrastructure Security	🟧	■	■
Physical Security	■	■	■

□ Enterprise Responsibility ■ Cloud Provider Responsibility

🟧 Shared Responsibility

Figure 41 Responsibility for security depending on the type of cloud service.[1.]

How to Assess the Security of a Cloud Service?

The best tool to assess the security of a cloud solution is risk analysis. It enables you to identify and assess the risk:

- prior to entering a cloud service,
- during its duration,
- in the event of its cancellation or changing of the provider.

In practice, you should prepare a risk analysis that is as thorough as possible prior to entering a cloud service, and subsequently supplement it with new threats or their assessment resulting from changes in the services over the course of the service, and always take into consideration the option to cancel it or to change the provider. When combing through materials on cloud security available online, you will encounter an opinion, expressed not just by marketers, that entering cloud services reduce (mitigate) the risks involved in information security. However, this refers to reducing the business risk (profit vs. cost) in the case of developing or testing of new solutions and technologies required by the business. In a cloud, the infrastructure is available on demand; you do not waste any time on purchasing, transporting and putting it into the Data Center, or on configuring it. Test data, which are anonymised or insensitive from the company's perspective, are sufficient to perform a business assessment of such a solution. The impact of a leak of invulnerable (non-confidential or anonymised) data is small (very low or low) and its likelihood in the case of popular providers does not exceed the average value. This combination creates a low or medium risk and a significantly high chance to create and test new services.

In order to conform to the legal requirements (the Act on Personal Data Protection and the Act on the National Cybersecurity System), companies implement Information Security Management Systems based upon ISO 27001, which requires that a risk analysis be performed when assessing the security of new services. In the case of cloud services, an example of such an analysis is provided by The European Network and Information Security Agency (ENISA), in its risk analysis presented in Cloud Computing Benefits, risks and recommendations for information security[3].

That is version 2.0. However, it is worth looking through the previous one. It presents a list of vulnerabilities and exposed resources assigned to individual risks.

The updated version of the document contains the following list of the most significant risks:

1. Loss of governance: Loss of governance: in using cloud infrastructures, the client necessarily cedes control to the Cloud Provider (CP) on a number of issues that may affect security. At the same time, SLAs may not offer a commitment to provide such services on the part of the cloud provider, thus leaving a gap in security defences. This also includes compliance risks, because investment in achieving certification (e.g., industry standard or regulatory requirements) may be put at risk by migration to the cloud. This also includes compliance risks. The main cloud providers demonstrate compliance with the security certificates, i.e.: ISO 27001, ISO 27017, ISO 27018, SOC 2, SOC 3, and PCI DSS, however, this is usually at the IaaS services level. SaaS service providers tend not to have such certificates.
2. Lock-in: there still is little on offer in the way of tools, procedures or standard data formats or services interfaces that could guarantee data, application and service portability. This can make it difficult for the customer to migrate from one provider to another or migrate data and services back to an in-house IT environment.
3. Isolation failure. The Provider's cloud resources are used to serve multiple customers using the multi-tenant model. This risk category covers the failure of mechanisms separating storage, memory, routing and reputation between different tenants (an attack against a single customer of the service may affect another). However it should be considered that attacks on resource isolation mechanisms (e.g., against hypervisors) are still less numerous and much more difficult for an attacker to put in practice compared to attacks on traditional operating systems.
4. Management interface compromise: Customer management interfaces of a public cloud provider are accessible through the Internet and mediate access to larger sets of resources (than traditional hosting providers) and therefore pose an increased risk, especially when combined with remote access and web browser vulnerabilities.
5. Data protection. Cloud computing poses several data protection risks for cloud customers and providers. In some cases, it may be difficult for the cloud customer (in its role as data controller) to effectively check the data handling practices of the cloud provider and thus to be sure that the data is handled in a lawful way. This problem is exacerbated in cases of multiple transfers of data, e.g., hybrid clouds.

[1] Adam Gordon: The Official (ISC)2 Guide to the CCSP CBK 2nd Edition (Responsibility Depending on the Type of Cloud Services)

[2] https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

[3] https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security

6. Insecure or incomplete data deletion. When a request to delete a cloud resource is made, as with most operating systems, this may not result in true wiping of the data. Adequate or timely data deletion may also be impossible (or undesirable from a customer perspective), either because extra copies of data are stored but are not available, or because the disk to be destroyed also stores data from other clients. In the case of multiple tenancies and the reuse of hardware resources, this represents a higher risk to the customer than with dedicated hardware.
7. Malicious insider. Cloud architectures necessitate certain roles which are extremely high-risk. Examples include the Cloud Provider's system administrators and managed security service providers. The mali ciousness of their actions has an impact not only on the Cloud Provider, but also on its customers.
8. Customers' security expectations. The perception of Security levels by Customers might differentiate from the actual security (and availability) offered by the Cloud Provider, or the actual temptation of the Cloud Provider to reduce costs further by sacrificing on some security aspects.
9. Availability Chain. Reliance on Internet Connectivity at Customer's end is greatly beneficial, but it creates a Single point of failure in many cases, particularly in politically unstable countries. Determination of the cause of unavailability of the services may also create conflicts between the Cloud Provider and Customer if it is uncertain which side is at fault.

Summary

Understanding of the definitions, characteristics, deployment methods and types of the services is essential to the understanding of the cloud security issues. You can use the information available at the websites of: Cloud Security Alliance, NIST, ISACA, ISC2, and ISSA. However, before you use a cloud service, it is worth performing a risk analysis. You can find a sample one in Cloud Computing Benefits, risks and recommendations for information security. Of course, the risks identified and assessed there must be adapted to the service being analysed as well as to the risk matrix used at your company.

Jarosław Stawiany

> ”
>
> **Understanding of the definitions, characteristics, deployment methods and types of the services is essential to the understanding of the cloud security issues.**

7.13 Secure routing

The activities of telecom operators and IP traffic exchange points do not come down just to providing simple connectivity between users. The role of the service providing subject is way broader. It's responsible for the upkeep and maintenance of network, it should conduct constant monitoring, ensure the capacity and supply, development, coordination of cooperation and activities of subsequent large traffic users. It is also responsible for router security.

What is routing?

Routing is a process of establishing a route for packages in a network and sending network traffic through it. We have several dozen thousand subjects possessing their own **autonomous system number** in the World Wide Web – usually, they are internet operators, and large content providers. Every AS number has its **IP address classes** assigned, and they're managed by particular operators. This means that as a rule, all classes assigned to an operator are subject to one, coherent **routing policy**. Each operator has its own rules of roaming, and announces them (through all the networks it keeps an exchange of traffic with) to other operators in the internet. For routing information exchange, the **BGP protocol** (Border Gateway Protocol) is used. This protocol requires starting a TCP session to exchange information between neighbours, meaning routers exchanging information directly between each other (the so-called **BGP session**). Within this session, information about networks broadcasted by a particular AS, as well as information on visibility, status, and situation of its neighbours is being sent between operators. Each of the operators can, to some extent, modify the information sent, and thus influence the route of packages in the network. This is natural, and it serves to enforce the operator's routing policy to. This way, an operator can optimize the manner of package routing with e.g. differences in quality of its connections, and their prices in mind, or apply more elaborate policies according to the needs of the business it runs. Basing on information acquired regularly from all its BGP sessions, operator's routers build their own version of a **BGP table**, meaning available routing paths between particular AS systems around the world. This is the so-called full (some say: worldwide) BGP table. Basing on information from that table, alongside with information acquired from external routing protocols, information on local routings, available interfaces and their addressing – each router builds its own **routing table**, according to which it directs packages between available network interfaces. Also, **route servers** are useful in managing BGP sessions. They are used in e.g. **internet exchange points** (e.g. **TPIX**), to make managing BGP sessions easier. Thanks to that, the number of sessions may be reduced, information aggregated, and routing decisions made easier. It may be easily said that the BGP protocol along with bases informing about IP address assignation (e.g. **RIPE-DB**) are absolutely fundamental for the modern internet to function.

How to understand routing security?

In the case of routing information exchange, security can have different dimensions:

Availability	A condition necessary for routing based on BGP I the proper visibility of neighbours, meaning maintaining routing information exchange through BGP sessions. A longer lack of communication results in the BGP session breaking (the so-called BGP flap) and as a result, the loss of facility to exchange network traffic with a certain connection, and the necessity of recalculating routing path tables, and redirecting the traffic to available backup routes (if such are available).
Integrity	Integrity, meaning coherence and correctness of the routing information exchanged is fundamental to the BGP protocol. Operators have to trust that routing information coming from their peers (other operators with whom they exchange traffic) are correct. Injecting faulty information to a BGP table may have far reaching implications, often affecting the whole internet within range of particular traffic. There are two kinds of errors – they may stem form mistakes, or from the operator's routers not functioning properly (without deliberate conduct), or from intentional, conscious effort aiming to change (interfere with) the routing.

Accountability

Accountability should be understood as the facility to recover infor-mation about who and when distributed routing information of a cer-tain type. This allows reacting to emerging errors, and preventing future errors.

Non-repudiation

In case of routing, non-repudiation should be understood as the certainty that the party with which we exchange information about routing is the actual subject we have in mind. Also, attacks on non-repudiation include IP address spoofing, consisting in generating IP packages with a fake source address (oftentimes a random one, or one pointing to a certain target – the victim).

With each of these aspects, one can imagine scenarios of an attack. Cases like that are known to have occurred in networks.

According to data ISOC from the years 2017 and 2018:

- Statistically, around 10% autonomous systems a year is affected by some problem related to routing security.

- In 2017, 13935 routing incidents occurred in the World Wide Web. Data for the year 2018 show an increase in their number (while this text was being written, the data for 2018 has not yet been prepared by ISOC, we will publish it as soon as it's available on our website: cert.orange.pl).

The most characteristic network routing problems are[4]:

Event	Explanation	Consequences	Example
Prefix/Route Hijacking	A network operator or an attacker impersonates another operator, pretending that the server or a network is its client.	Packages are being sent to a wrong location, and may cause Denial of Service (DoS) kind of attacks or interception of traffic.	2008 YouTube hijack April 2018 Amazon Route 53 hijack attacks
Route leak	Network operator with many internet providers (oftentimes due to an accidental misconfiguration), informs one internet provider in possession of a route to a certain destination through another provider.	May be used for MITM attacks, including traffic inspection, modification and reconnaissance.	September 2014. VolumeDrive begun to announce almost all BGP paths which it has learnt from Cogent to Atrato, causing disruption of traffic in places as distant from the USA as Pakistan and Bulgaria.
IP Address Spoofing	Someone creates packages with a fake IP address to hide the sender's identity or to impersonate someone else	The main cause of DDoS Reflection type of attacks	March 31, 2018 Akamai reported an amplified DDoS attack with the use of memory buffering mechanism Memcached of 1.3Tb/s

[4] On the basis of the ISOC report.

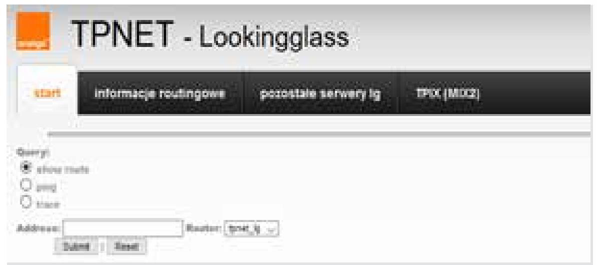
What does the situation in Poland look like?

Ironically, the situation in Poland looks quite well as compared to the rest of the world. It is like this due to several reasons:

1. The existence of mechanisms such as prefix-automat in the TPNET network, which for years have been forcing correct labelling of announced IP addresses in the RIPE-DB database. Without a RIPE-DB database correctly filled out, the exchange of BGP traffic with the Orange network not possible. Because the Orange network is the largest internet provider in Poland, in practice this means that the correctness of **RIPE-DB in the field of addressing in Poland is close to 100% (a score unattainable for other countries).**
2. The community of people in charge of IP traffic exchange in Poland is relatively small (we have slightly over 200 autonomous systems), they possess high competences and as an addition, they know each other, and they cooperate. This cooperation is the condition of the internet functioning properly, so business and competition related issues, or any other kind of issues apart from technological ones, cannot interfere with technical communication. The small number of people minimizes the possibility of mistakes, allowing an unknown subject into the traffic, or allowing activities that were not agreed upon by the community.
3. Large operators in Poland use anti-spoofing filters in their networks. This means that very little traffic with incorrect source addresses appears in Polish networks.
4. In Poland, large operators have NOC and CERT teams at their disposal, monitoring and managing 24/7, which allows quick reaction to potential errors and issues.
5. The IT market in Poland can be easily called mature – there are no new subjects suddenly appearing here, which could affect the structure and routing in the network in any significant way.
6. We have a limited quantity of well-managed, large internet exchange points (e.g. TPIX), which makes managing routing easier and more efficient.

What can I do, for the network I manage to be more secure?

As Orange Polska we also actively monitor the state of routing, and we possess logging systems announcing routing path changes. We also provide tools, such as e.g.: http://lg.tpnet.pl/. They are meant to make checking network status and available routes easier.

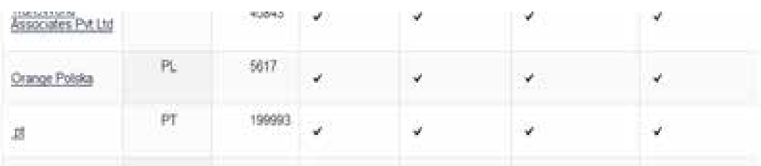


We also manage one of the biggest internet exchange points in Poland – TPIX, and we invite everyone to connect (http://www.tpix.pl/):

Orange Polska is the first subject in Poland, which became a member of the **MANRS: Mutually Agreed Norms for Routing Security initiative.** We actively promote this kind of endeavours during events we organize (e.g. European CERT meeting in May 2018), as well as during large, country-wide conferences (e.g. PLNOG, also in 2018).

If you care for the security of your network – definitely join the initiative. MANRS membership comes down to implementation (or confirmation of application) certain simple rules in the field of network management and configuration, which increase the level of security. Among the important things are the correctness and timeliness of RIPE-DB database entries, presence of anti-spoofing filters, correctness of routing paths aggregation (minimization of the number of the paths without losing the quality of information) and other. The appropriate audit then verifies the operator's level of compliance (in terms of configuration and procedures) with recommendations, and confirms the accordance with MANRS guidelines, or recommends taking corrective action. After fulfilling the requirements and passing the audit – the operator is put on the list of secure subjects.

More information about the joining procedure, requirements, and the initiative itself can be found on the cert.orange.pl website as well as at the source – on the ISOC website: http://www.manrs.org/.



Associates Pvt Ltd		40845	✓	✓	✓	✓
Orange Polska	PL	5617	✓	✓	✓	✓
.pt	PT	199993	✓	✓	✓	✓

Andrzej Karpiński
Director of Security Architecture and Development for ICT,
Orange Polska

7.14 Security in the company - do I need an IDM system?

The English acronym IDM, derived from Identity Management means identity management. This solution often includes the management of access to the (Identity and Access Management, IAM) systems, and these terms are often used interchangeably.

What is identity?

Identity is a set of features that define a person as a unit. This concept derived from philosophy means identicalness, which should be understood as an unambiguous definition of unchangeable information about a person. The English term for identity IDENTITY, like the Polish word IDENTICAL, come from the Latin IDEM meaning “the same”. By saving unambiguous information that identifies the identity of a person, we never lose sight of it.

For example, in Poland, for official purposes, the PESEL number is a unique identifier of identity, thanks to which offices, despite the change of a surname, address or hair color, should be able to unambiguously determine the person concerned.

The same applies to enterprises. We need to know who we are employing - each IT system should record data allowing to identify a person who has gained access to it and carried out specific activities in it. It can be clearly indicated who and to what extent had access to data. Logs from such operations should go to the SIEM system.

From employment to dismissal, i.e. managing the access to systems

When a new person appears in a company, it is advisable to be pre-determined in advance as to what is available to him/her in a given post at the moment of employment. It can be fixed assets (computer, desk, telephone) as well as access to IT systems. And here comes the second function of the IDM system, i.e. access management. Fast, often automatic authorization in systems used by an employed person is a great facilitation, but at the same time a potential threat - it is an easy access to company data, especially in cases where there are no well-defined ranges of profiles assigned to a given position and granting rights takes place discretionarily. In the case of people changing the position or place of employment in the company structure (HR-type migrations, accounting, or customer service and IT), you can quickly adjust privileges to new obligations, grant those necessary or revoke redundant ones. A similar procedure takes place when a person leaves the company. Automating such tasks is the primary benefit of using IDM. All of this is done in order not to tempt such a person to use data that should not be available to them, or - what is equally important - to limit the possibility of conducting an attack by a cybercriminal who will take over the access accounts of such an employee.

Theory vs practice

The implementation of IDM requires the involvement of the entire company, because the problem affects all the processes supported by IT systems. Therefore, all areas must actively participate in the implementation of such a solution. The project of IDM implementation may encounter many difficulties such as:

- lack of system standardization, for example in the scope of logging in - a login assigned in the system or local password interception
- lack of system standardization, for example in the scope of logging in - a login assigned in the system or local password interception
- various technologies of supported systems and the necessity of creating separate connectors
- focusing on full-time employees and, as a result, no prospects for external employees - suppliers or people collaborating on the basis of contracts which are not supported by the HR process (B2B, internships)
- conflicting interests of IT and business, i.e. security versus convenience.

Problems must be identified and solved prior to the implementation, because their appearance in the course of implementation may extend it or cause a partial implementation that will not ensure the full use of the tool in terms of both security and convenience of use. While technical problems can be overcome with an appropriate amount of work and financial resources, the last point is the issue of the company’s internal policy. It’s the management team that needs to make everyone understand that IDM implementation will be a common success that will bring benefits.
The benefits clearly defined and described for each area should be acceptance criteria for the perception of the implementation.

Although IDM implementation is a finite and one-off process, ensuring security - including access management - is a continuous process that requires constant support.

Does it protect the company?

- Thanks to the existence of records of granted access, data between IDM and events in the systems obtained by SIEM can be correlated on an ongoing basis and security incidents can be detected (e.g. an attempt to gain access to a system non-authorized in a given position, or specific operations carried out after working hours).
- The 2016 Cloud Security Alliance[5] survey reported that 22% of attacks are done by obtaining employee’s credentials. In the case | of properly defined and supervised access, the scope of an attack is effectively limited by a specific list of systems available to the employee.
- The Newtrix[6] report [2] of 2018 states that current or former employees are the ones responsible for the majority of data theft incidents. That is why, it is so important that the access is never excessive and received immediately after the employee leaves the company.

Maciej Domański

[5] https://www.esecurityplanet.com/network-security/22-percent-of-data-breaches-are-caused-by-compromised-credentials.html
[6] https://www.netwrix.com/2018itrisksreport.html

7.15 Psychology and phishing

Why are we so easily deceived?

24 hours. If we consider the fact that we spend 1/3 of the day on sleep, there are 16 hours left when we function at higher or lower speed. These are 960 minutes, during which we usually get first information just after waking up after we have picked up our mobile phone. After that, we receive information from advertisements on the radio, news on the Internet or TV, conversations with friends, by browsing social media or carrying out tasks at work. There is too much of it. The fact that we do not lose our heads due to the multitude of information from around us is thanks to our brain. Evolution has taught the brain to "take shortcuts", which on the one hand is beneficial for us on a daily basis, but on the other hand - being aware of this helps cybercriminals, too. They are people who want to steal our logins, passwords or sensitive data in order to get rich quickly and easily. And they are fully aware of how easy it is to deceive our brain.

Heuristics in anti-virus, heuristics in brain

If you have ever observed the mechanisms behind the anti-virus software, the concept of heuristics[7] is not new to you. If an anti-virus wrongly identifies a file as a malicious one, it will end up with a false positive, which will not cause much damage. However, in the case of the brain it is not so easy. If the brain uses heuristics, the moment we realize that we have wrongly identified a given situation, it may turn out - and most often it will be so - that it is too late. In such a case, it will not end up with a false positive, but the damage will probably be much greater.

Why does our brain choose to take a shortcut? At a high level - in order to avoid being flooded with information (which has been mentioned above), at the lower level - to avoid the situation, in which one is unable to decide what to do. Let's bring the situation to the lowest possible level.
We enter a shop and choose... let's say a sausage. We do not happen to analyze in detail the composition of each sausage, the percentage of meat, the nature of fillers... If one likes Podwawelska sausage, the vast majority of us will simply buy Podwawelska sausage! After all, nobody thinks about it. Our brain simply helps us with the choice at the subconscious level. In complete independence from us.

"Such e-mails have already been"

Let's take examples of the most popular phishings from last year:

- "An invoice" from the telecommunications service provider
- a piece of information about a paid courier package (with a large amount of money)

If we regularly receive invoices from our provider, why should this one be different? Recall how often you actually look at the e-mail that you have just received. What may go wrong? It's from Orange, the pictures are the same, the date is similar. By associating the incoming e-mail with similar messages we receive, the brain will not waste energy to think about whether it is really true. Is it an exaggeration? So, think about what will happen when the alleged sender of the message is a company whose services you have never used? The reaction will be completely different. You will think: "Are they crazy?" And your attention will be focused on the appearance and content of the e-mail, which will help you detect the fraud immediately.

Effective coping with phishing requires a lot of self-control, and the "perpetrator" is heuristics of representativeness, which makes us "classify an object on the basis of its similarity to a typical case that we know"[8].

"I did not pay anything at all?!"

E-mails "from couriers" are one of the most popular scams in recent years. Criminals, however, adapt to the growing awareness of users, reaching for more and more sophisticated psychological tricks. Admit it yourselves - the way "to confirm sending a parcel" does not work on as many people anymore, and the situation, in which we get an e-mail about a parcel we did not order, makes us laugh. What if we receive an e-mail about the parcel, which we have already paid? What is worse, it "cost" us several thousand zlotys? We'll click on the link right away, because it can still be withdrawn!
And here comes the heuristics of accessibility, which consists in "assigning greater probability to events that are easily available to consciousness and / or characterized by strong emotions". Because on the Internet there is so much news about people having been robbed online and a friend of a friend has been, too! Even worse if the theft with the use of the Internet happened to someone in our family, which makes it even more credible in our eyes (or rather - of course subconsciously - in our brains) that we have to save ourselves quickly! The effect will, of course, be the opposite.

How to deal with it?

Certainly, do not give up using the Internet and do not demonize the risks connected with it, because they do not change the fact that the Internet facilitates our daily lives greatly. The major way seems to be getting rid of automatism. Over the last dozen or so years, we've moved a significant part of ourselves to the network - moreover, it has become so automatic that we need to think about it before we realize how much we do online. Be careful and in case of doubts, do not be ashamed to consult someone who is better at "the Internet stuff".
And do not read long information quickly, or when we're tired. Nothing will happen if we wait until the morning, the world will not end. Just make a habit of simply slowing down in all potentially suspicious situations. A few more minutes a day can save you many days of stress.

Michał Rosiak

> **E-mails "from couriers" are one of the most popular scams in recent years. Criminals, however, adapt to the growing awareness of users, reaching for more and more sophisticated psychological tricks.**

[7] https://www.esecurityplanet.com/network-security/22-percent-of-data-breaches-are-caused-by-compromised-credentials.html
[8] https://www.netwrix.com/2018itrisksreport.html

7.16 Security management in the DevOps model

In the recent years, running IT projects in the DevOps mode (development and operations) has gained tremendous popularity, which is still growing I is sufficient to look at the number of job offers for the position of DevOps Engineer). The main goal of this methodology is to combine software development areas and operator (administrative) roles to improve communication between these teams. The effect is the direct translation into the delivery time of a new solution and implementation of changes in production environments.

As early as 2011 Amazon boasted about making changes to production environments on average every 11.6 seconds (which gives almost 7,500 changes a day)[9]. A large number of tools developed over the recent years that support both project organization, communication, testing, automation and constant integration lies behind these figures. It introduces many new possibilities like the automation of operations, e.g. the creation of a new virtual machine, its configuration, and finally placing applications on it. These actions are repetitive and executed by the same mechanism, so the risk of making a mistake in the configuration that may cause the malfunction or security vulnerability in this area is minimal. Provided that the automatic machine has an implemented verification - whether the image of system is up-to-date and whether the libraries that were included do not have published security vulnerabilities. Another one should be verification of the operation and security improvement, i.e. hardening of the operating system and making sure that the application which will be launched is adequately secure. With such a pace of introducing changes to IT environments, it's hard to imagine testers who would verify with each change the way in which the application works. Unfortunately, the development speed of security tools is not so fast, and certainly not of those available in the OpenSource mode. IT security is frequently not taken into account when creating tools that automate work, and if they do, they cover a small area of the problem.

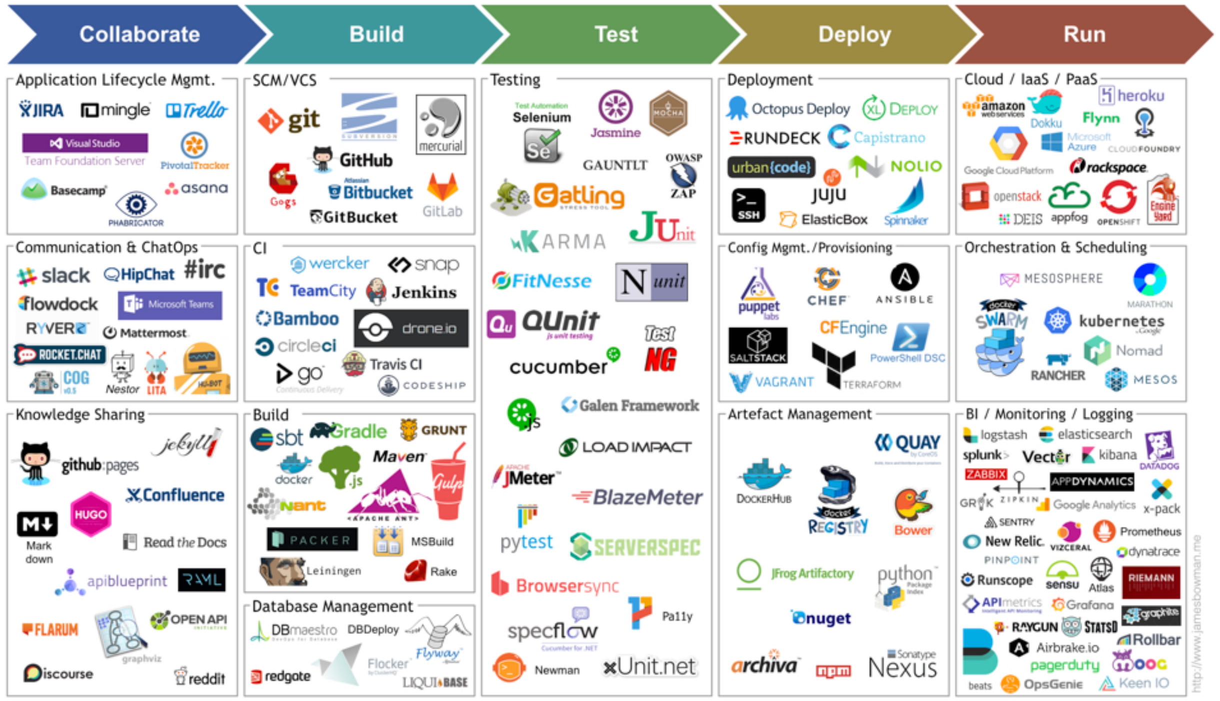


Figure 42 *Ecosystem of DevOps Tools*[10].

This is clearly visible in Graph 42, where the life cycle of the change in the DevOps model has been presented. Often the only place where ICT security is taken into account is the implementation stage, at which security tests or an appropriate audit are performed.

The earlier we realize that this approach is not sufficient, the better it is for our company. Especially that the described methodology describes both a few areas that are particularly vulnerable to attacks and allows the addition of mechanisms that ensure security in a generic way. Starting with solutions that allow you to manage vulnerabilities in the layer of the operating system, installed libraries and applications (including application servers), ending with scripts verifying environmental configurations, e.g. CIS Benchmark[11]. Please note that not all security violations should break the software delivery chain. In special cases, risks related to detected vulnerabilities can be mitigated by automatic configuration of WAF (Web Application Firewall) solutions in accordance with the increasingly emerging Security as a Code paradigm.

SAST (Static Application Security Testing) and DAST (Dynamic Application Security Testing) scanners will introduce a significant value into the software delivery chain. Static scanners, frequent source code analysis in terms of security vulnerabilities, can be triggered every time a merge request is made by a programmer. As a result, the most critical errors will not even reach the production code repository which will prevent them from further propagation in the project. Dynamic scanners can be configured at the same time at which functionality tests are launched. It will often help avoid problems related to proper configuration of tools, so that the authentication in the application takes place in an appropriate way - test scripts already have information about the active session and user context, all you need to do is use them for another purpose. Programmers under pressure of time often ignore recommendations or leave issues related to ICT security for later. And there is a lot to watch out for. According to the analysis carried out by Orange Polska, 400 potential vulnerabilities are introduced into averagely 10,000 code lines.

Graph 38 lists most commonly found vulnerabilities in the source code for applications created in JAVA and PHP technologies and mobile applications dedicated for the Android platform. About 100 applications were analyzed, which included web applications, APIs and mobile applications. One of the most common vulnerabilities is Weak XML Schema, which consists of many errors in the implementation of SOAP API. Such programming interfaces are often used by legacy-type systems, which significantly hinders its complete removal. The presence of the vulnerabilities associated with encryption - Weak Encryption and Insecure SSL - on the list is certainly alarming. The first vulnerability refers to the use of weak algorithms to create, for example, OTP passwords, while the other one often involves excluding the verification of the host certification path with which the application establishes (or receives) a connection. These are vulnerabilities that are extremely easy to improve and which significantly affect the security level of the solution.

Log Forging
Weak XML Schema
Cross Site Scripting
Mass Assigment: Request Parameters Bound into
Persisted Objects/ Insecure Binder Configuration
Unreleased Resource: Streams/Sockets
Path manipulation
Dynamic Code Evaluation: Unsefe Deserialization/
Code Injection
XML External Entity Injection
Privacy Violation
Insecure Cookies
Header Manipulation
HTTP Parameter Pollution
Open Redirect
Server-Side Request Forgery
Insecure SSL: Overly Board Certificate Trust
Weak Encryption: Insecure Mode of Operation
JSON injection

Figure 43 *Most commonly found vulnerabilities in the app source code.*

Methodologies such as DevOps in the following years will gain even more popularity. The way of managing vulnerabilities in such environments must evolve adequately so that organizations consciously manage security. It is no longer enough to periodically test specific solutions or configure several scanners so that they perform defined tests. It is necessary to integrate with the tools used in the process of software delivery and to have at least one mechanism in each of the chains.

Grzegorz Siewruk

[9] O'Reilly Conference Velocity, 2011 –Jon Jenkins "Velocity Culture"
[10] Bowman, James. 2017. "Continuous delivery tool landscape." January 30. Accessed 2018-12-15.
[11] https://github.com/topics/cis-benchmark

7.17 Tyre pressure sensor analysis

Since November 2014 car manufacturers are obliged to equip new vehicles in tyre pressure sensors. The Tyre Pressure Monitoring System (TPMS) – is usually composed of sensors installed in the wheels and an electronic central unit gathering measurements and signalling potential anomalies to the car's computer and the driver.

The rationale behind the TPMS systems points to the following benefits:

- security (maintaining the right pressure ensures proper traction, stability, and optimal braking distance)
- economy and ecology (too low a pressure causes increased tyre wear and fuel consumption)
- saving time during exploitation (option to monitor pressure without connecting the wheel to a manometer).

Figure 44 *TPMS system logotype.*

The literature mentions two kinds of TPMS solutions: direct and indirect. The indirect method, which is not covered in this article, uses elements of the ABS to estimate the radius of the wheel under strain, which is dependent on internal pressure.
The direct method uses the wheel sensors, usually integrated with a valve, which send a report about pressure to the TPMS central unit by radio.
The article deals with the signal analysis and the construction of device meant for intercepting those signals and sending their own (sensor emulation).

Sensors - recognition

In the TPMS system recognition phase used in Toyota vehicles, information found on the internet has been used. Parts used in Japanese vehicles are in 99% made in Japan (Pacific Industrial Co.), which is why the amount of information available is smaller than of European made solutions.
It was decided not to remove a wheel from an operational vehicle. Online auctions and the pictures included in them are a source of valuable information, and such was the case here. In addition, manufacturers of TPMS diagnostic devices provide a lot of information on the types of sensors used in specific make and model of cars, as well as on manufacturers themselves. Because of that, it wasn't hard to find a picture with a visible FCC number. Thanks to American fondness for sharing information, basic information on the sensors can be found on FCC websites.

Interception

For detection and preliminary identification of TPMS sensor signals a RTL-SDR was used, meaning a cheap radio tuner. Many solutions were tested, but in the end, the identification was conducted an open source project https://github.com/jboone/gr-tpms. The project includes tools for both inter-ception and analysis of signals – especially the modulation used (FSK), measuring bit rate and frequency deviation, as well as for establishing package length, and then CRC parameters (trigger value and polynomial mask) using the brute force method.

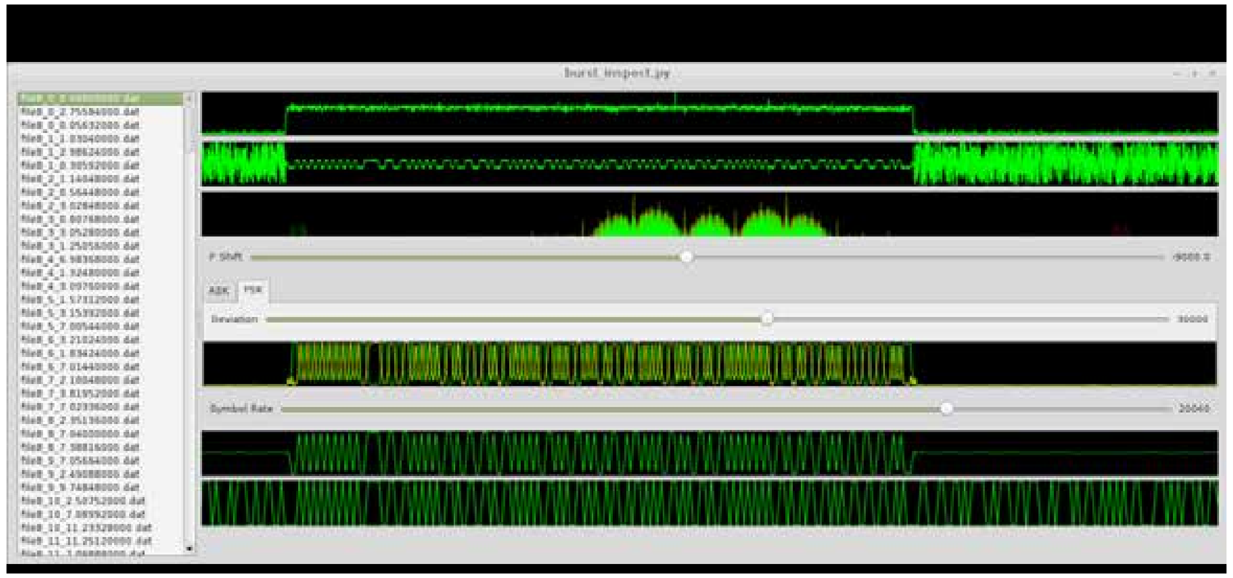


Figure 45 *Burst_inspect tool for analysing FSK modulation parameters*

The original wheel sensors send out data around every minute, regardless of whether the vehicle is moving or if it's parked. The loss of a few packages of data is not signalled to the driver, it takes as much as 20 minutes of no data being sent to make the TPMS system to actually report the issue.

Signal analysis

With the use of the tools described above (with some modifications, since Japanese sensors are a little exotic, and there was no support for them in the tools used) example samples for all four sensors were obtained (some of the identifiers were hidden under X symbols; HEX and binary values):

```
XX XX X3 18 CC 97 80 66 0B
XXXXXXXX XXXXXXXX XXXX0011 00011000 11001100 10010111 10000000 01100110 00001011
XX XX X3 31 CB 98 00 68 AD
XXXXXXXX XXXXXXXX XXXX0011 00110001 11001011 10011000 00000000 01101000 10101101
XX XX X3 32 D1 9B 03 5C FE
XXXXXXXX XXXXXXXX XXXX0011 00110010 11010001 10011011 00000011 01011100 11111110
XX XX X2 F3 D3 1B 03 59 D6
XXXXXXXX XXXXXXXX XXXX0010 11110011 11010011 00011011 00000011 01011001 11010110
```

Hardware

The idea was that the tool for intercepting and sending TPMS signals be simple, cheap, and energy-efficient. The Banana PI tandem (a minicomputer similar to Raspberry PI) and RTL-SDR, located in close proximity of the car did not manage to fulfil those requirements. The choice fell to the Arduino platform. RFM69 transceiver was chosen as transmitter and receiver for the 433MHz band, controlled by a SPI interface. With the knowledge of modulation used, frequency value, bitrate and deviation, one can easily program an appropriate operating mode for the module's receiver and transmitter, basing on the RMF69 module documentation.

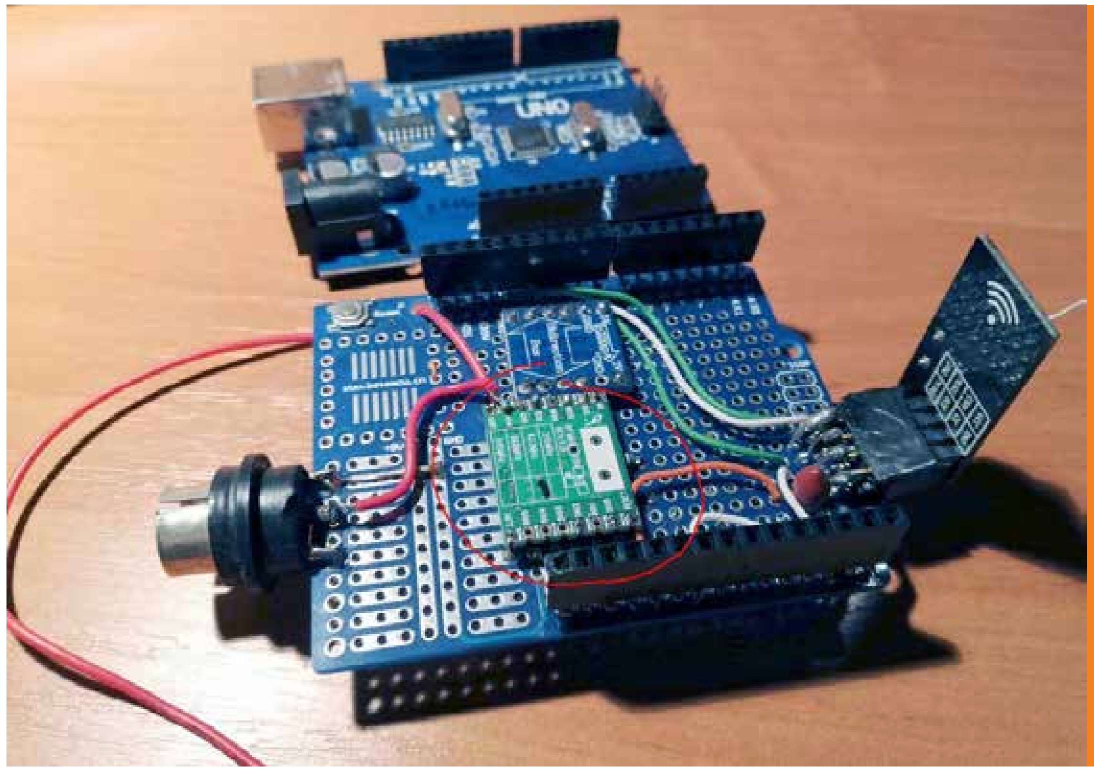


Figure 45 *Shield prototype with RFM69 radio.*

The programmed module allows both receiving and transmitting data packages compatible with the TPMS system. The whole thing is managed with the help of a program for Arduino, communicates through a serial link. Located on the prototype board for Arduino Uno, is the mentioned radio module (in the centre, green) as well as a voltage converter (Arduino UNO uses 5V logic and power supply, module RMF69 3.3v).

Using this device, it is possible to easily repeat the intercepted samples as well as to create our own packages with a correct control sum. Because the transmitted parameters and their location within the packages were still unknown, a simple TPMS programmer was used for reading the previously intercepted data packages:

```
XXX331     7°C    208KPa   (2,08 bar,   2,05 atm,   30 PSI)
XXX318     6°C    212KPa   (2,12 bar,   2,09 atm,   30,7 PSI)
XXX332    13°C    228KPa   (2,28 bar,   2,25 atm,   33 PSI)
XXX2F3    13°C    234KPa   (2,34 bar,   2,31 atm,   34 PSI)
```

Using trial and error, the location of the data in the packages was found (currently, the package format is available on the internet, but such information was not available when the analysis was being conducted). In the end, the package format was determined (first wheel, ID1-ID3 – unique sensor identifier):

meaning	ID1	ID2	ID3	?	Pressure *1.71-50	Temperature-40	?(e.g 7x'0')	^Pressure	CRC8
bits	XXXXXXXX	XXXXXXXX	XXXXXXXX	1	PPPPPPPP	TTTTTTTT	0000000		
example	XXXXXXXX	XXXXXXXX	XXXX0011	1	10011001	00101111	0000000	01100110	00001011
value					**153*1.71-50≈212**	**47-40=7**			

An option to manipulate bytes responsible for pressure and temperature values, as well as for displaying the values from the intercepted packages in a readable way using a serial console, was implemented in the program for Arduino.

Target device and its functions

Arduino Uno with proto shield is still too large and inconvenient for "field use" if, for example, one wants to put it in one's pocket. This is why the target device uses Arduino Pro Mini, version 8MHz/3.3V, transceiver RFM69 and for convenient wireless communication – the HC-05 Bluetooth module. The entire device is contained in a small plastic casing, which also includes two LR6 batteries.

A Bluetooth HC-05 module (profile SPP Bluetooth) was connected to the serial console, making it possible to display the intercepted TPMS packages of owned and surrounding Toyota cars (with a correct CRC sum and valid pressure and temperature values) through e.g. a phone with a Bluetooth console application installed (TerminalBT). The application also allows the modification of pressure and temperature value parameters and sending signals modified in this manner. The application meant to be developed for convenient use of the device through a smartphone which was not created due to the lack of time.

An example attack – correct pressure simulation

One of the attack scenarios tested, was sending fabricated packages with correct pressure in the wheel at an increased frequency (every second). In the meantime, the original sensor in the wheel reported low pressure values with the frequency of one package per minute. The TPMS system would not report the loss of pressure in the wheel. Only after the sending of the false packages would cease, the pressure loss indicator would light up and the driver was informed about the problem.

An inverse attack is also possible. Despite correct pressure in the wheels, one can cause the TPMS indicator to light up, by sending packages with a low pressure value at a high frequency. Most probably, the driver will stop to check on the tyres. This may be used e.g. to rob the driver in a remote location the "flat tyre" style.

In the test example, normal pressure equalled (according to the manual) 220-240 kPa. In the test, lowering pressure to a value below 187 kPa caused a problem with pressure to be reported (the TPMS indicator on the dashboard would light up in orange). Pressure value above 201 kPa caused the TPMS alarm to stop. Hysteresis of around 20kPa prevents the indicator from lighting up in lower, but acceptable pressure values.

Both cases present the possibility of cheating the TPMS system, and as a result, the driver. In the first case, it causes real danger – e.g. a valve slightly unscrewed by the attacker causes loss of pressure, which is being masked by a sensor emulator attached to the car. The loss of stable driving trajectory, and performing manoeuvres with the pressure significantly decreased created a serious hazard on the road, especially at higher speed.

Summary

Transmitting data by radio without proper security measures poses risk of interception, modification and jamming, meaning it doesn't fulfil any of the basic security requirements (Security Triad - CIA – confidentiality, integrity, availability). The work [1] points out to privacy threats, connected i.a. with vehicle identification with the use of unique wheel identifiers. Our own research (using SDR and an antenna for the 433MHz band and the prototype described) demonstrated the possibility of receiving the signal from tyres from several dozen meters, and successful transmitting modified signals from at least a dozen meters. This allows easily generating false pressure loss alarms in the victim's car wheels.

Another conclusion is that in Toyota's TPMS RAV4 system (4th generation), rotating tyres doesn't matter, as change in location of a wheel will not affect the system's functionality. This matters because sometimes one can meet with recommendation to rotate wheels every season, to ensure they wear evenly. The paid sensor system reconfiguration is not necessary in connection with such operation.

Konrad Kamiński

Literature

1. Ishtiaq Roufa i inni „Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study"
2. https://github.com/jboone/gr-tpms
3. RFM69 module documentation https://www.hoperf.com/data/upload/portal/20181127/5bfcb767eb0f2.pdf
4. Bluetooth console application https://play.google.com/store/apps/details?id=main.terminalBT

> ”
>
> **Three years ago, four Polish teams belonged to the European CERT Organisation. Today there are 18 such teams, 8 of them are accredited teams and the host of this publication – CERT Orange Polska – is a certified team.**

Partner's Commentary

Mirosław Maj
More than 20 years of experience in ICT security. Founder and president of the Cybersecurity Foundation, CEO of the ComCERT company, a former leader of CERT Polska team. In 2017-2018 he was the adviser to the Minister of National Defence of Polska on planning cyberdefence capabilities and building organizational structures as well as establishing international cooperation on the field of cyberdefence. Initiator of Polish Civic Cyberdefence organization. He is the member of Trusted Introducer team being responsible for accreditation and certification of CERTs. European Network Information Security Agency expert and co-author of many ENISA publications including CERT exercises and papers on improvement the CERT coordination. He organized cyber exercises in Poland and Georgia for energy, banking and telecommunication sectors. Speaker on many international conferences including the FIRST conferences. He is also the organiser of five editions of the cyber exercises Cyber-EXE Polska and SECURITY CASE STUDY conference.

Writing of summaries of cybersecurity-related phenomena is becoming increasingly difficult in each subsequent period of time. It is turning into systematic documentation of similar phenomena. We are observing an increasing number of incidents and discussing all those "Stuxnets", "Estonias", "WannaCries" and "Petyas, NotPetyas". Again and again, we have to admit that what has proved the most dangerous had not been foreseen and console ourselves that maybe at least this will have the positive side effect of someone noticing and finally doing something about it. And then we are disappointed.

All of that resembles a discussion held for the umpteenth time at a conference, when someone stands up and resentfully states that people are unaware of cyberspace threats; someone stands up after them and says that is why education is the most important; finally, a third one stands up and says that unfortunately, education does not work. Some people's frustration is growing, which is probably unnecessary.
What to do, how to live? That is a question which we often ask ourselves during each episode of the Foundation's podcast "Cyber, Cyber". Well, you just have to keep doing your job. In fact – you must keep doing your job, as there is some serious evidence that it is working quite well.

Few people know that the Act on the National Cybersecurity System, adopted in 2018, had practically been in development for nearly 10 years, and those who had begun the work on it also assisted in the drafting of its final text. Few people know that three years ago, four Polish teams belonged to the European CERT Organisation, whereas today there are 18 (!) such teams. Moreover, 8 of them are accredited teams and the host of this publication – CERT Orange Polska – is a certified team, which will likely be joined before the end of this year by another three Polish teams. This means that Poland is going to have the most such teams in Europe! Hardly anyone remembers that 10 years ago, today's largest Polish cybersecurity portals were in their infancy, whereas now Niebezpiecznik, Sekurak and Zaufana Trzecia Strona have tens or even hundreds of thousands of regular readers. Others, through their determination, are creating the first cybersecurity-related study programmes at Polish universities of technology.

All of that means that solid foundations for cybersecurity in Poland are being laid. I think that we cannot see this yet because, frankly speaking, those foundations still lack a solid structure on top of them. Last year's act of parliament gives us a chance that such a structure will come into being. It is important that we do not forget to expand and reinforce the foundations whilst being mindful of that process and participating in it. Let precise and no-nonsense regulations be created for the act of parliament, but at the same time, let us also build more CERTs, organise cybersecurity in sectors, propagate honest knowledge of cybersecurity and educate new cybersecurity graduates at our universities. That effort will certainly not be in vain.

8 How to protect financial institutions or companies, both large and small – Orange Polska security services

The increasing use of ICT systems in all aspects of running a business causes an increase in value of information, and as a result, the necessity to efficiently protect it. Here reaction time to potential threats that could affect our business counts. Orange Polska offers services, thanks to which you can minimize the risk in case of many kinds of threats.

The Internet of Things permeates our daily lives, and the threats associated with it are more and more noticeable. This is a challenge, especially due to the low security level of "smart" devices and the risk to use them for DDoS attacks (Distributed Denial of Service). As conducting these types of attacks is very expensive, we can expect a growing market for solutions offering "as-a-service" attacks.
Cybercriminals are becoming more cunning and ruthless. To counteract them, companies need to cooperate with security experts.
Orange Polska offers services that minimize the cyber risk pertaining to various threats.

Protection from DDoS attacks

What are DDoS (Distributed Denial of Service) attacks: A dispersed attack, meant to block access to resources, most commonly:

- attacks on the bandwidth necessary for providing a service, e.g. ICMP/UDP,
- attacks aiming to deplete systems resources e.g. TCP SYN,
- attacks on applications, e.g. attacks using the http, DNS, or VoIP applications protocols.

When to use: Unavailability of service.

What it's about: Protection of the customer's online resources from volumetric denial of service attacks. Network traffic is monitored 24/7/365 for anomaly detection. In case of an actual attack, we filter out the suspicious packages, so only normal network traffic reaches the customer. Used as a support for the solution Flow Spec mechanisms introduced into Orange networks, allow interception and mitigation of volumetric attacks of very large scale.

How it works: It is a combination of three elements: SOC and CERT Orange Polska teams, Arbor Networks platform, and the use of operator mechanisms in domestic and international traffic (dnssinkholing, blackholing etc.).

For whom: For everyone using the World Wide Web network (WWW) and possessing their own infrastructure

Benefits:

- Ensuring security of business processes and information
- Constant monitoring of traffic and identification of occurrence of potential threats
- Competences of Operational Security Centre experts available 24/7/365
- Immediate defence against attacks at the customer's infrastructure
- No need to invest in adequate infrastructure and flexible accounting model, thanks to cloud computing.

Firewall (Orange Network Security, Manageable UTM)

What it's about: There are two main components that increases customers' security:

- Next Generation Firewall system design for protection of incoming and outgoing traffic
- Service management portal for the customer

How it works: Access control for the customer's infrastructure and use of the internet through employees without the need to install additional security tools. Tools for application control and web filtering decide on the types of applications and categories of pages that are available to users.

For whom: For everyone using the internet and having their own infrastructure.

Benefits:

- Secure internet access
- No need to invest in IT security devices;
- Centralized security policy for all protected localizations

email Protection

What it's about: Customer's e-mail protection from threats such as infections, phishing, spam and data exfiltration.

How it works: Based on the platform managed in the Orange Polska network. The functionalities of this service are:

- Anty malware
- Anty phishing
- Anty spam
- Anty wirus
- DLP

For whom: For all the customers using e-mail

Benefits:

- Protection of the information sent via e-mail
- No need to invest in IT security devices;
- Centralized security policy for all protected localizations

MDM

What is it: Mobile Device Management is a solution for management of customer mobile device fleet.

What it's about: Monitoring and management of customer's mobile devices such as smartphones, tablets.

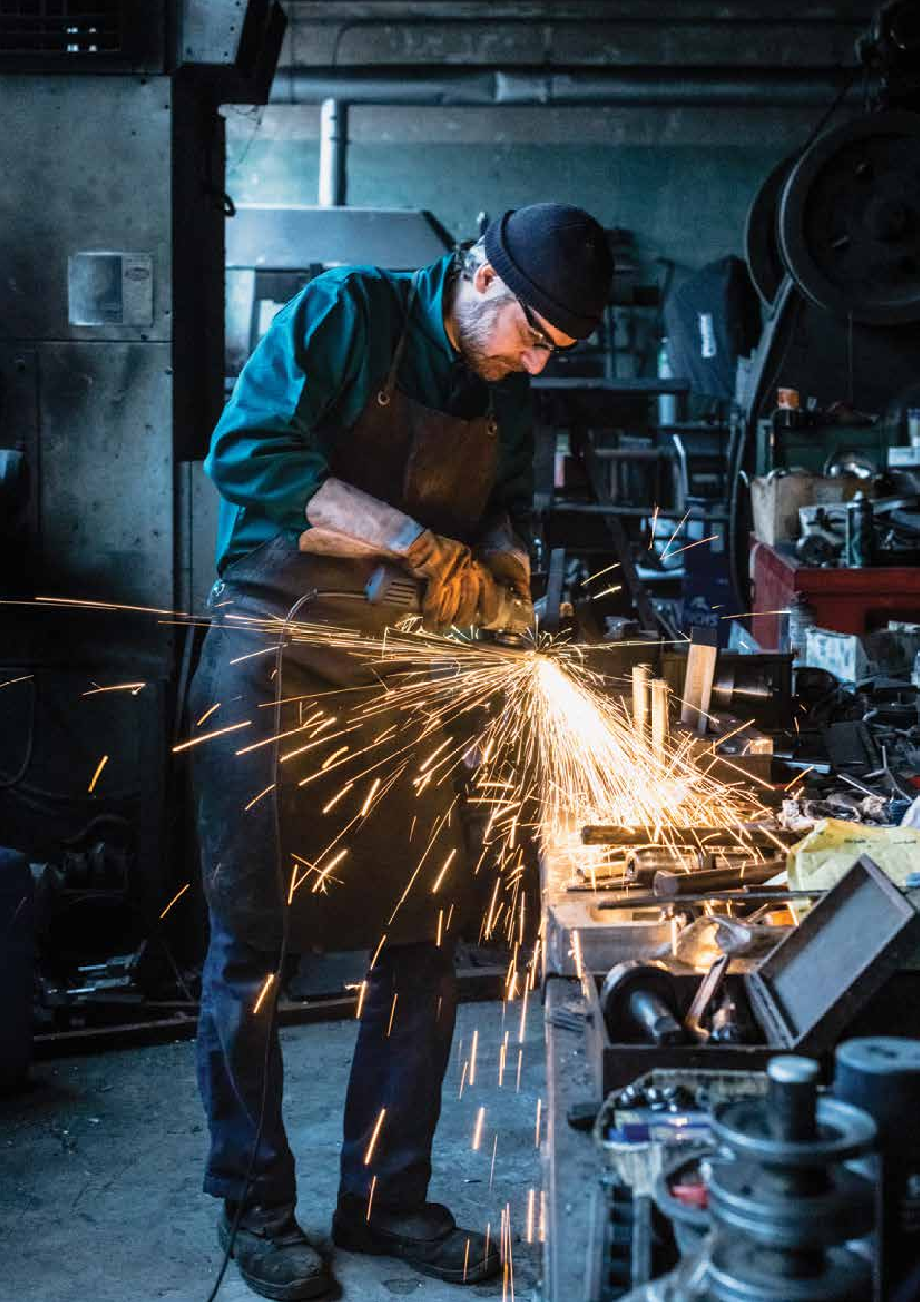
How it works:

- Managing mobile fleet from the console
- Centralised management of:
  - o Mobile devices – localisation, configuration, backup, remote blocking, data erasing
  - o Applications – central repo of applications, remote distribution and installation for users group
  - o backing up processes for the most important data stored on the mobile device
  - o security policies
  - o remote technical support

For whom: For those who manage mobile fleet (smartphones, tablets, laptops).

Benefits:

- Centralized mobile devices management in the company
- Standardisation



Monitoring security incidents

What is it: A constant process of identifying incidents, and notifying people responsible for managing the infrastructure

What it's about: By searching information about suspicious events (incidents) in the logs of the systems monitored

Available solutions applicable separately or in packages :

SIEM as a Service

When to use: If you want to be able to identify incidents in the whole infrastructure, keep data in a place and manage it efficiently

What it's about: Implementation or sharing the functionality of the SIEM system with the customer, in order to gather significant events from systems, applications, and their correlations, and search them for security incidents

How it works: Achoice of an appropriate system for the customer's needs and budget, delivery of a complete solution, which means its installation, availability and monitoring 24/7/365, integration of log sources, formulation and implementation of security scenarios

For whom: For everyone responsible for infrastructure and data maintenance

Benefits:

- Constant monitoring and identification of security incidents
- Immediate notification of people responsible for the infrastructure and protected data about
- Flexible tailor-made model, i.e. option of running it at the customer's place, or in a cloud

SOC as a Service

When to use: If you want to centralize security operations to quickly react to potential threats.

What it's about: A pre-made incident monitoring process, using competences of the Security Operations Centre (SOC) Orange Polska team – cyber-security operators, analysers and experts monitoring the customer's systems and data through e.g. SIEM.

How it works: A process involving integrating data from the customer's systems (a console, SIEM system data and other) with a rapid incident response team.

For whom: For everyone responsible for infrastructure and data maintenance, as well as for people bound by the regulations concerning quick response to incidents (e.g. RODO, KNF)

Benefits:

- A pre-formulated process of incident processing
- An experienced team of experts ready for work
- Lower costs – no need of building a team of specialists and competences from scratch
- Immediate notification about incidents

Feed as a Service

What is it: A compendium of knowledge concerning threats identified by CERT Orange Polska in the cyberspace, especially in the Orange Polska network

What it's about: Delivery of information about malicious activity observed on the internet, especially in the Orange Polska network (malware, C&C, other).

How it works: An automated process of information delivery as CSV text files, or API mechanisms in defined formats, containing data about so-called C&C servers, domains and IP addresses of web services infecting browsers with malicious software, IP addresses exhibiting malicious activity towards Orange Polska network (scanning ports, attack attempts etc.).

For whom: All organizations maintaining security systems

Benefits:

- Reinforcing the systems possessed with unique data gathered by CERT Orange Polska.

Vulnerability tests

What is it: Detecting and classifying the customer's system's vulnerabilities, which may be used for taking over it, stealing sensitive data, and other actions leading to image and financial losses.

When to use: In order to check the system's vulnerability to potential threats

What it's about: Using the knowledge and experience of CERT Orange Polska (White Hat Hacker), specialist software, which scans the customer's infrastructure, and generates a report with a list of detected vulnerabilities. Basing upon it, the CERT Orange Polska experts will prepare a list of the most important recommendations that should be implemented to avoid the use of the vulnerabilities by potential offenders.

For whom: Organizations possessing their own ICT infrastructure

Benefits:

- Evaluation and quick identification of security gaps and expert recommendations concerning improvement of the customer's infrastructure's security

Penetration tests

What is it: Practical evaluation of the current security status, especially the presence of known vulnerabilities, and resistance to security breach attempts

When to use: In order to test security mechanisms in the customer's infrastructure

What it's about: An attempt to gain unauthorized access to the customer's chosen ICT system, using the white box/ black box method

For whom: Organizations providing their infrastructure to other parties in the web

Benefits:

- Evaluation and quick identification of security gaps and expert recommendations concerning improvement of the customer's infrastructure's security
- Objective and independent evaluation of factual level of the system's security.

Performance tests

What is it: A controlled DoS/ DDoS type attack at the chosen elements of the customer's ICT system (network link, servers, services, internet node) conducted in order to evaluate the resistance to DDoS type attacks.

What it's about: Analysis conducted from the viewpoint of a potential offender, using the team's competences, traffic generators, pre-formulated scenarios of network attacks, and the transport network of the Orange Polska infrastructure

When to use: In order to test the security measures against DDoS type attacks

For whom: Organizations providing their infrastructure to other parties in the web

Benefits:

- Quick system security evaluation concerning DDoS type attacks
- Recommendations CERT Orange Polska concerning improvement of the system's security
- Objective and independent evaluation of factual level of the system's security.
- The option to define individual scenarios with the customer

Malware Protection InLine

What is it: Protection of the customer's network resources by preventing and detecting malware infections attempting to permeate to the client's infrastructure from the internet

What it's about: The customer's traffic at the Internet Point of Presence is monitored and analysed for the presence of malicious code in the files.

How it works: Malware is detected using techniques connected with detailed analysis of an attack. Suspicious network flows are reconstructed in virtual machines conducting advanced analyses of malware behaviour in an environment simulating the actual customer's environment (Sandbox).
The process is based on behavioural analysis of code, which also allows identifying advanced (APT) attacks and zero-day malware.
The customer's infrastructure's outgoing traffic is analysed for the connection of malware with the so-called C&C servers.

For whom: For everyone using the World Wide Web network and possessing their own infrastructure

Benefits:

- Quick identification and blockade of malicious software activity
- Protection from new-generation cyber-security threats of the APT and zero-day type
- No need of investing in service-protecting devices
- Protection from the customer's employees carelessness

Malicious software analysis

What is it: An analysis of malicious software delivered by a CERT Orange Polska customer as a part of a service.

What it's about: Behaviour evaluation concerning the malicious activities observed, (i.a. establishing IP addresses of Command&Control servers, IP addresses of domains), of the code delivered by the customer, by running it in a series of strictly controlled virtual environments of Orange Polska.

How it works: The result of the Orange Polska's analysis is a report from works describing the detected threats of malware's malicious activity in the system, along with the description of methods of its propagation.

For whom: For customers who want to check their software for an eventual occurrence of maliciousness, and become aware of its influence over the infrastructure

Benefits:

- Availability of the CERT Orange Polska's team and laboratory
- A report concerning the identified maliciousness, and its influence over the customer's infrastructure
- Recommendations of CERT Orange Polska concerning threat minimization

Secure DNS

What is it: Prevention of the consequences of a DDoS type attacks aimed at the customer's DNS infrastructure

What it's about: Geographical dispersion of the servers responsible for the customers' DNS. The queries always end up in the geographically (network-wise) closest server.

How it works: Orange Polska uses the "anycast" technology – tested and proven on the internet since many years. Worldwide networks providing the .com and .pl domains are functioning in this technology. SecureDNS consists of over 40 nodes, located in the Orange network, as well as other networks in Polska, and abroad, across five continents. The responses from the closest node will come with maximum speed, through shortest possible route, without delay.

For whom: For customers providing online services, internet domains owners

Benefits:

- Redirecting attacks from the customer's own infrastructure to DNS servers.
- Increasing the availability of DNS services
- Quick and easy service configuration, as well as handling of changes
- Geo-locarion of responses
- Option to fully outsource the customer's DNS service using the SecureDNS infrastructure.

Stop Phishing

What is it: Blocking traffic network coming from a phishing website created by a cyber-criminal

What it's about: Minimization of the consequences of phishing attacks, especially blocking network traffic to identified phishing websites, aimed at the customer's web service users (e.g. home-banking).

How it works: An active blockade of network traffic between Orange Polska network users, and servers or domains identified as elements of a phishing campaign. By using the SOC and CERT Orange Polska team, we can guarantee a swift blockade of the campaign, and notification of other rapid-response teams about the identified (CERT teams, alternative operators).

For whom: For customers providing online services (e-commerce)

Benefits:
- Minimization of the scale of attack by reducing the number of potential victims
- Lowering the costs of incident processing on the customer's side
- Significant reduction in the image risk connected with the customer's brand.

Web Application Firewall (WAF aaS)

What is it WAF: Web Application Firewall platform is located in the backbone network of jest Orange Polska

When to use: Unavailability of services connected with the customer's application

What it's about: Protection of the customer's resources form application attacks. The entire http/https traffic from the internet to the protected resources is being redirected to a service platform, and subjected to analysis according to the established security policy.

How it works: It allows protection from the most critical web application threats defined in OWASP Top 10, and allows increasing the security of web applications without the necessity of modifying their code.

For whom: For everyone using the World Wide Web, and possessing their own infrastructure

Benefits:
- Ensuring the security of information and business processes
- Constant monitoring of traffic and identification of occurrence of potential threats
- Competences of the Operational Security Centre experts available 24/7/365
- Immediate defence against attacks at the customer's infrastructure
- No need to invest in adequate infrastructure and flexible accounting model, thanks to cloud computing

CyberTarcza as a Service

What is it: Mobile devices protection for customers operating in the Orange Polska network against malware and phishing campaigns.

What it's about: Network traffic is monitored and analysed for potential cyber threats. The service blocks connections to the infected sites and pages according to categories defined by the customer.

How it works: Basis on the operator's internet traffic analysis, regardless the operating system

Functionalities:
- Anti-malware, anti-phishing
- Possibility to define locks at various times for employees and family;

CyberTarcza contains additional cyber threat intelligence developed for the customer and allows user to manage filters from over 30 categories.

For whom: For everyone using the Orange Polska mobile network including: consumer, entrepreneur, prepaid.

Benefits:
- Possibility of filtering;
- Protecion from Advanced Persistent Threats and zero-days;
- No need to invest in IT security devices;
- Protection from carelessness of the employees.

> CyberTarcza contains additional cyber threat intelligence developed for the customer and allows user to manage filters from over 30 categories.

9. Dictionary

AaS (ang. as a service) – an abbreviation that refers to services provided to the customer via the Internet.

Abuse – misuse of some capabilities of the Internet, i.e. inconsistent with the purpose or the law. Internet abuses include: network attacks, spam, viruses, illegal content, phishing, etc. An Abuse Team is a unit responsible for receiving and handling reported cases of abuse.

ACK "acknowledge" - one of the TCP flags set to confirm the network connection.

Adres IP (ang. IP address) – IP address (Internet Protocol address) a unique number for each device (e.g. computer) on the Internet, allowing its unambiguous identification in the network.

DNS Adress – used for naming devices on the Internet. It consists of domain names separated by periods. It is convenient for users and uses DNS hierarchical structure to translate it into IP address that is understandable for devices on the network.

Backdoor – "back door"; a vulnerability of the computer system created purposely in order to obtain later access to the system. A backdoor can be created by breaking into the system either by some vulnerability in the software or running a Trojan unknowingly by the user.

Blackholing from "black hole" – an action of redirecting network traffic to such IP addresses on the Internet where it can be neutralized without informing the sender that the data did not reach its destination.

Bot from "robot" – an infected computer that is taken over and performs the attacker's commands.

Botnet – "network of bots" – infected computers remotely controlled by an attacker. Botnets are typically used to run massive DDoS attacks or send spam.

C&C (*ang. Command and Control*) servers – an infrastructure of servers that is operated by cybercriminals, used to remotely send commands and control botnets.

CERT/CSIRT (*Computer Emergency Response Team, Computer Security Incident Response Team*) – a computer incident response team. The main task of CERT is quick response to reported cases of threats and violations of network security. The right to use the name CERT have only teams that meet very high requirements.

CISSP (*ang. Certified Information Systems Security Professional*) – an internationally recognized certificate confirming the knowledge, skills and competences in the field of network security.

Datagram - a block of data sent between computers on the Internet.

DDoS (*ang. Distributed Denial of Service*) – a network attack that involves sending to a target system such amount of data which the system is not able to handle. The aim of the attack is to block the availability of network resources. A DDoS attack uses multiple computers and multiple network connections, which distinguishes it from a DoS attack that uses a single computer and a single Internet connection.

DNS (*ang. Domain Name System*) - a protocol for assigning domain names to IP addresses. This system has been created for the convenience of Internet users. The Internet is based on IP addresses, not domain names, therefore, it requires DNS to map domain names into IP addresses.

DNS address – used for naming devices on the Internet. It consists of domain names separated by periods. It is convenient for users and uses DNS hierarchical structure to translate it into IP address that is understandable for devices on the network.

DNS sinkhole – DNS server that sends false information, making impossible to connect the target website(s). It can be used to detect and block malicious network traffic.

Domain name – a name of a domain; used in the URL to identify the addresses of websites. Examples of domains are .gov, .org, com.pl.

Exploit – a program that allows an attacker to take control over the computer system by exploiting vulnerabilities in operating systems and software.

Exploit 0-day– 0-day exploit - an exploit that appears immediately after the information about the vulnerability is published and for which a patch is not yet prepared.

Exploit kit – software that is run on servers, whose purpose is to detect vulnerabilities.

Firewall – software (device) whose main function is to monitor and filter traffic between a computer (or a local area network) and the Internet. Firewall can prevent from many attacks, allowing early detection of intrusion attempts and blocking unwanted traffic.

Honeypot – "honey pot"; a trap system, that aims at detecting attempts of unauthorized access to a computer system or data acquisition. It often consists of a computer and a separate local area network, which together pretend to be a real network but in fact are isolated and properly secured. From the outside, a honeypot gives an impression as if it contained data or resources attractive from the point of view of a potential intruder.

HTTP (Hypertext Transfer Protocol) – a communication protocol used by the World Wide Web. It performs as a so-called request-response protocol, e.g. when a user types an URL in the browser, then the HTTP request is sent to the server. The server provides resources such as HTML and other files and returns them as a response.

HTTPS (*Hypertext Transfer Protocol Secure*) – a secure communication protocol, which is an extension of the HTTP protocol and enables the secure exchange of information by encrypting data using SSL. When using a secure HTTPS, a web address begins with "https: //".

ICMP (*Internet Control Message Protocol*) – a protocol for transmitting messages about the irregularities in the functioning of the IP network, and other control information. One of the programs that uses this protocol is ping that let a user check whether there is a connection to another computer on the network.

IDS (Intrusion Detection System) – a device or software that monitors network traffic, detects and notifies about the identified threats or intrusions.

Incident – an event that threaten or violate the security of the Internet. Incidents include: intrusion or an attempt of intrusion into computer systems, DDoS attacks, spam, distributing malware, and other violations of the rules that apply to the Internet.

IoT (*Internet of Things*) - concept of a system for collecting, processing and exchanging data between "intelligent" devices, via a computer network. The IoT includes: household appliances, buildings, vehicles, etc.

IP (*Internet Protocol*) – a unique number for each device (e.g. computer) on the Internet, allowing its unambiguous identification in the network. IPS (Intrusion Prevention System) - a system that detects threats and prevents attacks in real time.

IPS (*Intrusion Prevention System*) – a system that detects threats and prevents attacks in real time.

Keylogger – a program that operates in secret and logs the information entered via the keyboard. It is used to track activities and capture sensitive user data (i.e. passwords, credit card numbers).

Malware (*malicious sofware*) – software aimed at malicious activity directed at a computer user. Malware include: computer viruses, worms, Trojan horses, spyware.

MSISDN (*ang. Mobile Station International Subscriber Directory Number*) – phone number; a subscriber number in mobile network stored on the SIM card and in the registry of subscribers.

OWASP (*ang. Open Web Application Security Project*) – the global association whose main idea is to improve the security of Web applications.

Phishing – a type of Internet scam whose goal is to steal the user's identity, i.e. such sensitive data that allows cybercriminals to impersonate the victim (e.g. passwords, personal data). Phishing occurs as the result of actions performed by the unconscious user: opening malicious attachments or clicking on a fake link.

Port scanning - action of sending data (TCP or UDP) to a specific computer system on the network. It enables to get information about the operation of certain services and opening of certain ports. Scanning is typically performed in order to check the security or it precedes an intrusion.

Ransomware – a type of malware, which when installed on a victim's system encrypts files making them inaccessible. Decryption requires paying a ransom to cybercriminals.

Rootkit – a program whose task is to hide the presence and activity of the malware from system security tools. A rootkit removes hidden programs from the list of processes and faciliate an attacker to gain unauthorized access to a computer.

RST (*reset*) – one of the TCP flags that resets the connection

SIEM (*Security Information and Event Management*) – a system for collecting, filtering and correlation of events from many different sources and converting them into valuable data from the security point of view.

Sinkholing (*hole*) – a redirection of unwanted network traffic generated by malware or botnets. Redirection can be done into the IP addresses where the network traffic can be analyzed, as well as into non-existent IP addresses.

Port scanning – action of sending data (TCP or UDP) to a specific computer system on the network. It enables to get information about the operation of certain services and opening of certain ports. Scanning is typically performed in order to check the security or it precedes an intrusion.

SLA (*Service Level Agreement*) – an agreement to provide services at the guaranteed level. SLA is agreed between the client and the service provider.

Sniffing – an action of eavesdropping and analysis of network traffic. Sniffing can be used for managing and troubleshooting the network administrators but also by cyber criminals to wire-tapping and interception of confidential information of users (e.g. passwords).

SOC (*ang. Security Operations Center*) – a security center that combines both technical and organizational functions, in which systems such as SIEM, anti-virus programs, IDS/IPS systems, firewalls, provide meaningful information to the central incident management system.

Spam – unsolicited and unwanted messages sent in bulk, usually using email. Messages of this type are usually sent anonymously using botnets. Most often spam messages advertise products or services.

Spyware (*spy software*) – spy software that is used to monitor actions of a computer user. The monitoring activity is carried out without consent and knowledge. The information collected includes: addresses of visited websites, email addresses, passwords or credit card numbers. Among spyware programs are adware, trojans and keyloggers.

SSL (*Secure Socket Layer*) – the security protocol to ensure the confidentiality and integrity of data and their authentication. Currently, the most commonly used version is SSLv3 that is considered as a standard for secure data exchange and developed under the name of TLS (Transport Layer Security).

SYN (*ang. synchronization*) – one of the TCP flags sent by the client to the server in order to initiate the connection.

SYN Flood - a popular network attack, whose main purpose is to block the services of the server. It uses TCP.

TCP (*Transmission Control Protocol*) – the connection protocol; one of the basic network protocols for controlling data transmission over the Internet. It requires connection between devices in the network and enables to obtain confirmation that data reached the destination.

Trojan – Trojan horse; a malicious program that enables cybercriminals to remotely take control of the computer system. An installation of a trojan on a user computer is usually done by running malicious applications download from untrusted websites or mailing attachments. Besides a remote command execution, a trojan can allow eavesdropping and intercepts user passwords.

UDP (*ang. User Datagram Protocol*) – a connectionless protocol, one of the basic network protocols. Unlike TCP, it does not require setting up the connection, observing sessions between devices and a confirmation that the data reached the destination. It is mostly used for transmission in real time.

URL (*Universal Resource Locator*) – the web address used to identify the servers and their resources. It is essential in many Internet protocols (e.g. HTTP).

VoIP (*Voice Over Internet Protocol*) – “Internet telephony”; a technique for transmitting speech via the Internet. Audio data is sent using the IP protocol.

Vulnerability – an error; feature of computer hardware or software that exposes a security risk. It can be exploited by an attacker if an appropriate fix (patch) is not installed.

Worm – a self-replicating malicious computer program. It spreads across networks, which is connected to the infected computer, using either vulnerabilities in the operating system or simply user’s naivety. Worms are able to destroy files, send spam, or acting as a backdoor or a Trojan horse.

For more information please visit:
www.cert.orange.pl